Tampereen yliopisto

JETTA VIRTANEN

KÄYTTÖLIITTYMÄN KÄYTTÄJÄN AUTENTIKOINTI RFID-TEKNOLOGIALLA

Diplomityö
Luonnontieteiden ja tekniikan tiedekunta
2020

TIIVISTELMÄ

Jetta Virtanen: Käyttöliittymän käyttäjän autentikointi RFID-teknologialla
Diplomityö
Tampereen yliopisto
Johtamisen ja tietotekniikan diplomi-insinöörin tutkinto-ohjelma
Tarkastajat: professori Sami Hyrynsalmi ja professori Marko Seppänen
Tammikuu 2020

Diplomityö on tehty Cimcorp Oy:lle. Diplomityön tarkoituksena oli tutkia, miten käyttäjän autentikointi ja käyttäjätunnusten hallinnointi varastonhallintajärjestelmässä voitaisiin toteuttaa yleistä teknologiaa hyväksi käyttäen. Tunnistautuminen ja tunnusten hallinnointi tapahtuisi toisessa palvelussa olemassa olevasta varastohallintajärjestelmästä erillään. Diplomityön tavoitteena oli kartoittaa nykyään monissa sovelluksissa laajasti käytössä olevaa RFID (Radio Frequency Identification) eli radiotaajuustunnistusta. Tekniikalla on monia etuja, mutta tietoturvallisuuden tasoa tulee parantaa salaustekniikkaa käyttämällä. Tutkimuksen päätavoitteena oli määrittää mahdollisuus käyttää teknologiaa varaston hallintajärjestelmässä ja toteuttaa Cimcorp Oy:n varastonhallintakäyttöliittymään käyttäjän autentikointi RFID-teknologialla.

Diplomityön tutkimuksen taustatiedot kerättiin olemassa olevien tutkimusten avulla. Työn teoriaosuus käsittelee lyhyesti keskitettyyn käyttäjähallintaan kehitettyjä autentikointimetodeja sekä työn tutkimuksen ja toteutuksen kohteeksi valitun RFID-autentikoinnin hyötyjä ja haittoja. Työssä on tarkasteltu tarkemmin tutkimuksen kohteeksi valitun LDAP-protokollan (Lightweight Directory Access Protocol) soveltuvuutta asiakkaan RFID-tunnisteiden rekisteröinnin ja ylläpidon keskittämiseksi LDAP-hakemistopalvelimelle eriytettynä Cimcorp Oy:n tietokannasta.

Diplomityön toiminnallisiin toteutuksiin lukeutuvat RFID-tunnisteen lukeminen työasemaan liitetyltä lukijalaitteelta sekä käyttäjän tunnistaminen LDAP-tietokannasta tunnisteen perusteella. Diplomityö sisältää kuvauksen LDAP-palvelinsovelluksen kehitysympäristöstä, toiminnasta sekä rakenteesta. Työn tuloksena käyttäjän autentikointi toteutettiin soveltuvalla RFID-tunnisteella käyttäen LDAP-teknologiaa varastonhallintaohjelmiston java-käyttöliittymässä. Käyttäjän on mahdollista kirjautua käyttöliittymäsovellukseen RFID-tunnisteen avulla.

Diplomityössä esitetään yhteenveto RFID-tekniikan soveltuvuudesta todennuksen ja pääsynhallinnan näkökohdista. Tutkimuksen tulosten perusteella voidaan päätellä, että RFID-järjestelmillä on monia käyttökelpoisia sovelluksia, mutta niiden käyttö voi aiheuttaa tietosuojauhkia.

Avainsanat: RFID, LDAP, käyttäjähallinta, autentikointi

ABSTRACT

Jetta Virtanen: User interface authentication with RFID technology
Master of Science Thesis
Tampere University
Master's Degree programme in Management and Information Technology
Supervisors: professor Sami Hyrynsalmi and professor Marko Seppänen
January 2020

The Master's thesis has been done for Cimcorp Automation Ltd. The purpose of this thesis was to study how user authentication and general user management in warehouse control system could be implemented using common technology. The identification management would be implemented in the other service separated from the existing warehouse management system. The aim of the thesis was to survey the RFID (Radio Frequency Identification) widely used in many applications today. The technology has many advantages, but the level of security should be improved by using encryption technology. The main goal of the study was to determine the possibility to use technology in the warehouse management system and to implement user authentication with RFID technology in Cimcorp Ltd. user interface.

Background information for the thesis research was collected through existing studies. The theoretical part of the thesis briefly discusses the advantages and disadvantages of authentication methods developed for centralized user management as well as the RFID authentication chosen for the research and implementation of the thesis. The applicability of the LDAP (Lightweight Directory Access Protocol) to centralize the registration and maintenance of RFID tags on a LDAP directory server has been further investigated.

Functional implementations of the thesis include reading the RFID tag from a reader device attached to the workstation and identifying the user from the LDAP database by the tag. The thesis contains a description of the development environment, operation and structure of the LDAP server application. As a result of this work, user authentication was performed with a suitable RFID tag using LDAP technology in the java interface of the warehouse management software. It is possible for the user to log in to the UI application using the RFID tag.

The thesis summarizes the applicability of RFID technology in the aspects of authentication and access management. The results of the study show that RFID systems have many useful applications, but their use may pose a security risk.

Keywords: RFID, LDAP, user management, authentication

ALKUSANAT

Tämä diplomityö on tehty Cimcorp Oy:lle vuonna 2019. Työn ohjaajana on toiminut professori Sami Hyrynsalmi. Cimcorp:in puolelta työn valvojana on toiminut Teemu Koskinen. Professori Marko Seppänen on toiminut työn toisena tarkastajana. Suuret kiitokset kaikille työn ohjauksesta sekä neuvoista ja kommenteista. Kiitokset myös muille Cimcorp:in työntekijöille, jotka ovat opastaneet ja neuvoneet työn eri vaiheissa.

Porissa, 2.2.2020

Jetta Virtanen

SISÄLLYS

TERMIT JA NIIDEN MÄÄRITELMÄT

APDU	Application Protocol Data Unit, viestintäyksikkö älykortinlukijan ja älykortin välillä.
ASN.1	Abstract Syntax Notation One, vakiomuotoinen käyttöliittymäkuvauskieli sellaisten datarakenteiden määrittelemiseksi, jotka voidaan järjestää monitasoisella tavalla. Sitä käytetään laajasti televiestinnässä ja tietokoneverkoissa ja erityisesti salauksessa.
CSP	Cryptographic Service Provider, ohjelmistokirjasto, joka toteuttaa koodaus- ja dekoodaustoiminnot, joita tietokonesovellusohjelmat voivat käyttää esimerkiksi vahvan käyttäjän todennuksen tai suojatun sähköpostin toteuttamiseen.
CSS	Cascading Style Sheets, tyyliohjejärjestelmä, joka sisältää useiden, eri lähteistä peräisin olevien tyyliohjeiden soveltamisen samanaikaisesti, tarkoin määriteltyjen preferenssisääntöjen mukaan.
DAP	Directory Access Protocol, hakemistojen käsittelyprotokolla.
DIT	Directory Information Tree, hakemistotiedon puumainen rakenne, joka koostuu LDAP-hakemiston tietueiden yksilöllisistä nimistä.
DN	Distinguished Name, hakemistotietueen yksilöllinen nimi.
DNS	Domain Name System, Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.
EEPROM	Electrically Erasable Programmable Read-Only Memory, puolijohdemuisti, jonka sisältö voidaan tyhjentää elektronisesti ja uudelleenkirjoittaa ohjelmallisesti.
EPC	Electronic Product Code, sähköinen tuotekoodi, joka on tallennettu RFID-tunnisteeseen.

GDPR	General Data Protection Regulation, EU:n yleinen tietosuoja-asetus, 2016/679.
HMAC	Hash-based Message Authentication Code, viestin avaimellinen hash-autentikointikoodi
IETF	The Internet Engineering Task Force, Internet-protokollien standardoinnista vastaava organisaatio.
ITU	International Telecommunication Union, Kansainvälinen televiestintäliitto on YK:n alainen televiestintäverkkoja ja -palveluja kansainvälisesti koordinoiva järjestö. ITU:n päätehtäviä ovat standardointi, radiotaajuuksien jakaminen ja puhelinverkkojen yhteyskäytäntöjen organisointi maiden välillä siten, että ulkomaanpuhelut ovat mahdollisia.
ISO	International Organization for Standardization, Kansainvälinen standardointijärjestö.
IEC	International Electrotechnical Commission, Kansainvälinen sähkötekninen toimikunta.
LDAP	Lightweight Directory Access Protocol, hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla.
LDIF	LDAP Data Interchange Format, vakio tekstidatan tiedonsiirtomuoto LDAP-luettelon sisällön ja päivityspyyntöjen esittämiseksi.
PKI	Public Key Infrastructure, julkisten avainten hallintajärjestelmä.
RFC	Request for Comments, IETF-organisaation julkaisemia Internetiä koskevia standardeja.
RFID	Radio Frequency Identification, radiotaajuinen etätunnistus.

RDN	Relative Distinguished Name, hakemistorakenteen RDN-nimissä käytetään suhteellista viittaustapaa, jonka avulla tiedot järjestetään puuhierarkiassa ylhäältä alaspäin.
SASL	Simple Authentication and Security Layer, kehys autentikointiin ja tietoturvaan Internet-protokollissa. Se irrottaa autentikointimekanismit sovellusprotokollista, jolloin teoriassa voidaan käyttää mitä tahansa SASL:n tukemaa autentikointimekanismia missä tahansa sovellusprotokollassa, joka käyttää SASL:ää.
SPOC	Single Point of Control, keskitetty hallinnointi.
SSL	Secure Sockets Layer, tietoverkkosalausprotokolla.
TCP/IP	Transmission Control Protocol / Internet Protocol, Internet-liikennöinnissä käytettävän tietoliikenneprotokollan yhdistelmä
TLS	Transport Layer Security, aiemmin tunnettu nimellä SSL, on salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.
UI	User Interface, laitteen tai ohjelmiston osa, jonka kautta käyttäjä käyttää laitetta.
UID	Unique Identifier, yksilöllinen tunniste

.

1. JOHDANTO

Diplomityö on tehty Cimcorp Oy:lle. Cimcorp Oy on automaatiojärjestelmien johtavia toimittajia rengas- ja elintarviketeollisuudelle sekä vähittäiskaupan ja postin jakelukeskuksiin. Yhtiön tarjoamat ratkaisut logistiikan ja tuotannon automatisointiin parantavat asiakkaiden toiminnan kannattavuutta ja kilpailukykyä. Ratkaisut perustuvat korkeatasoiseen omaan robotti- ja ohjelmistoteknologiaan sekä tuotteistettuihin palvelukonsepteihin. Yhtiö on toimittanut jo yli 5 000 robottiyksikköä vaativiin materiaalinkäsittelysovelluksiin.

Cimcorp Oy toimii kansainvälisillä markkinoilla. Yhtiön palveluksessa on 300 ammattilaista, jotka palvelevat asiakkaita monipuolisesti ja laaja-alaisesti automaatioalan ongelmien ratkaisussa. Yhtiöllä on pääkonttori Ulvilassa sekä tytäryhtiöt Kanadassa ja Yhdysvalloissa. Kotimaassa huoltoa tarjoavat toimipisteet sijaitsevat Helsingissä, Lahdessa ja Jyväskylässä. [1]

Diplomityön tarkoituksena oli tutkia, miten käyttäjän autentikointi ja käyttäjätunnusten hallinnointi varastonhallintajärjestelmässä voidaan toteuttaa ulkopuolista tunnistautumisjärjestelmää hyväksi käyttäen. Tunnistautuminen ja tunnusten hallinta tapahtuu toisessa palvelussa olemassa olevasta järjestelmästä erillään. Diplomityön tavoitteena oli kartoittaa nykyään monissa sovelluksissa laajasti käytössä olevaa RFID (Radio Frequency Identification) eli radiotaajuustunnistusta. Tekniikalla on monia etuja, mutta käytössä tulee ottaa huomioon myös tietoturva-kysymykset. Tietoturva- ja yksityisyysongelmien ratkaisemiseksi on käytettävä salaustekniikkaa. RFID-tekniikka käyttää sähkömagneettisia kenttiä etälukuun ja -tallentamiseen RFID-tunnisteilta. RFID-tunnisteet lähettävät ja vastaanottavat radiotaajuisia kyselyitä antennin avulla RFID-lähetin-vastaanottimelta. [2]

Tutkimuksen päätavoitteena oli määrittää mahdollisuus käyttää teknologiaa varaston hallintajärjestelmässä ja toteuttaa Cimcorp Oy:n varastonhallintakäyttöliittymään käyttäjän autentikointi RFID-teknologialla. Käyttäjän olisi mahdollista kirjautua varastonhallintajärjestelmän käyttöliittymäsovellukseen RFID-tunnisteen avulla, jolloin käyttöliittymän näkymä määräytyisi käyttäjälle asetetun roolin mukaiseksi. RFID-tunniste määräisi myös tuotantolaitoksen alueen tai laitteen, jossa käyttöliittymä toimii. Järjestelmän tulisi

ilmoittaa, mikäli jonkin toiminnan suorittaminen jää kiinni käyttöoikeuksista, ja antaa mahdollisuus samassa yhteydessä vaihtaa käyttäjää.

RFID-tunnistautuminen on nopeaa ja vaivatonta. Tunnisteita on saatavana erimuotoisina, -kokoisina, -tyyppisinä ja -materiaaleina. RFID-tunnisteet luetaan yleensä ilman virheitä. Useita tunnisteita voidaan lukea samanaikaisesti ja tunnisteiden tiedot voidaan uudelleenkirjoittaa. Luku onnistuu myös vaikeissa tai likaisissa ympäristöissä, mutta haittoja esiintyy, jos ne saatetaan kosketuksiin metallin tai nesteiden kanssa. [3]

RFID-tunnisteet sisältävät yksilöllisen tunnisteen ja ne voidaan lukea useiden metrien etäisyydeltä ilman optista tai visuaalista kosketusta. Nämä kaksi näkökohtaa tuovat esiin tietosuojakysymyksiä, erityisesti tunnisteiden jäljitettävyyden luvattomien osapuolten toimesta. [2]

Diplomityössä tutkittiin myös mikä olisi asiakkaan tietohallinnolle toiminnallinen web-sovellus, jonka avulla pystytään rekisteröimään ja ylläpitämään soveltuvia RFID-tunnisteita asiakkaan LDAP-hakemistopalvelimelle. LDAP-hakemistopalvelimelta henkilöön sidottua tunnistetietoa voisi mahdollisuuksien mukaan käyttää edelleen myös ulkoisissa järjestelmissä. Tällaisia voisivat olla esimerkiksi tuotantolaitoksen kulunvalvonta ja tulostuspalvelut. Integraation toteutus ei kuulunut tämän diplomityön sisältöön.

Sovelluksen toiminnallinen toteutus tapahtui Cimcorp Oy:n varastohallintajärjestelmässä, josta se on siirrettävissä LDAP-hakemistopalvelimen sekä java-sovelluksen omaavaan tuotantoympäristöön.

Tämän diplomityön tutkimuksen taustatiedot kerättiin olemassa olevien tutkimusten avulla. Työn teoriaosuus käsittelee lyhyesti keskitettyyn käyttäjähallintaan kehitettyjä autentikointi-metodeja sekä työn tutkimuksen ja toteutuksen kohteeksi valitun RFID-autentikoinnin hyötyjä ja haittoja. Työssä on tarkasteltu tarkemmin tutkimuksen kohteeksi valitun LDAP-protokollan (Lightweight Directory Access Protocol) soveltuvuutta asiakkaan RFID-tunnisteiden rekisteröinnin ja ylläpidon keskittämiseksi LDAP-hakemistopalvelimelle eriytettynä Cimcorp Oy:n tietokannasta.

Diplomityön toiminnallisiin toteutuksiin lukeutuvat RFID-tunnisteen lukeminen työasemaan liitetyltä lukijalaitteelta sekä käyttäjän tunnistaminen LDAP-tietokannasta tunnisteen perusteella. Diplomityö sisältää kuvauksen LDAP-palvelimen toteutuksesta ja sovelluksen kehitys-ympäristöstä, toiminnasta sekä rakenteesta. Työn tuloksena käyttäjän autentikointi toteutettiin soveltuvalla RFID-tunnisteella käyttäen LDAP-teknologiaa

Cimcorp Oy:n varastonhallintaohjelmiston java-käyttöliittymään. Käyttäjän on mahdollista kirjautua käyttöliittymäsovellukseen RFID-tunnisteen avulla.

Diplomityössä esitetään yhteenveto tekniikan soveltuvuudesta RFID-todennuksen ja pääsynhallinnan näkökohdista. Tämän tutkimuksen tulosten perusteella voidaan päätellä, että RFID-järjestelmillä on monia käyttökelpoisia sovelluksia, mutta niiden käyttö voi tuoda esiin joitain tietosuojauhkia.

RFID-järjestelmien käytössä on panostettava yrityksen ja yksilön yksityisyyden takaamiseen, estettävä tunnisteiden laiton seuranta, luvaton profilointi, kloonaaminen ja laiton lukeminen / kirjoittaminen. Yksi haittapuoli voi olla myös tekniikan käyttöönoton aiheuttamat lisäkustannukset. RFID-järjestelmä on kalliimpi kuin sisäänrakennettu tunnistusjärjestelmä. Järjestelmä vaatii alkuinvestointina erityyppisten lukijoiden ja tunnisteiden valinnan, hankinnan ja testauksen. Kustannukset voivat nousta edelleen, jos järjestelmää laajennetaan tiettyä mukautettua sovellusta kuten kulunvalvontaa varten.

Diplomityö rakentuu seuraavasti. Luku 2 tarkastelee lyhyesti digitaalista autentikointia sekä esittelee autentikointitekijät ja -tyypit. Luvussa käydään lävitse myös autentikoinnin uhat ja turvallisuusnäkökohdat. Luvussa 3 käsitellään Cimcorp:in varastonhallintajärjestelmän käyttöliittymän autentikoinnin nykyinen toteutus sekä esitetään varsinainen tutkintakysymys, miten käyttäjän autentikointi voitaisiin toteuttaa ulkopuolista tunnistautumisjärjestelmää hyväksi käyttäen. Luku 4 esittelee lyhyesti RFID-teknologian arkkitehtuurin, sovelluskohteet sekä RFID-järjestelmän suojauksen. Luvussa 5 syvennytään tarkastelemaan käyttäjähallinnan tueksi kehitetyistä standardeista ja protokollista erityisesti LDAP:ia. Diplomityö painottuu luvusta 6 lähtien LDAP:in käyttäjien hallinnan toteutukseen sekä varastonhallintajärjestelmän käyttäjäprofiileihin ja käytettäviin palvelinohjelmiin. Luvussa 7 esitetään käyttäjän tunnistuksen toteutus RDIF- teknologiaa ja LDAP-palvelinta hyödyntäen. Lopulta luku 8 kokoaa työn tulokset ja johtopäätökset yhteen.

2. DIGITAALINEN AUTENTIKOINTI

Digitaalinen autentikointi tarkoittaa sähköistä prosessia, joka mahdollistaa henkilön sähköisen tunnistamisen. Autentikointi voi myös lisäksi vahvistaa sähköisessä muodossa olevien tietojen alkuperän ja eheyden esimerkiksi myöntämällä digitaalisen varmenteen verkkosivuston aitouden osoittamiseksi. [4]

Digitaalinen todennus on prosessi, joka määrittyy tarpeesta todentaa yksittäiset ihmiset tai yhteisöt etäyhteyden kautta verkon yli. Todentamisen yleisenä tarkoituksena on vähentää petoksia tapauksissa, joissa henkilö väärinkäyttää henkilöllisyyttään tai käyttää toisen henkilön henkilöllisyyttä luvattomasti. Digitaalinen todennus tukee yksityisyyden suojaa vähentämällä luvattoman pääsyn riskejä yksilöiden tietoihin. [5]

2.1 Mitä on autentikointi

Autentikoinnissa kaksi osapuolta kommunikoi, ja toinen tai molemmat haluavat todeta henkilöllisyytensä toiselle saadakseen käyttöoikeuden suojattuihin resursseihin. Käyttäjän autentikoinnissa on kyseessä henkilön fyysinen henkilöllisyys eli käyttäjän todennus. Käyttäjän todennus on turvallisuusrakenteen keskeinen osa. Autentikointi toimii ovenvartijana muille turvallisuustehtäville, jotka [6]:

- varmistavat/rajoittavat tietojen saatavuuden valtuutetuille henkilöille
- varmistavat tietojen muuttamisen valtuutettujen henkilöiden kautta
- suorittavat toimenpiteiden jäljityksen.

Onnistunut todennus tarjoaa kohtuullisen riskittömän takuun siitä, että palveluun tällä hetkellä pyrkivä henkilö on sama kuin se, joka aiemmin käytti palvelua. Digitaalinen identiteetti on tekninen haaste, koska prosessiin sisältyy yleensä useiden henkilöiden varmentaminen verkon kautta. [5]

Protokolla on joukko vakiintuneita sääntöjä, jotka määräävät tietojen muotoilun, lähettämisen ja vastaanottamisen, jotta päätelaitteet voivat kommunikoida riippumatta niiden

rakenteiden tai standardien eroista. Jotta tiedot voidaan lähettää ja vastaanottaa onnistuneesti, viestinnän osapuolten on hyväksyttävä ja noudatettava protokollan sopimuksia. [4]

2.2 Autentikointitekijät ja -tyypit

Verkkokäyttäjän todentamisessa on olemassa kolme tekijäluokkaa, joita voidaan käyttää varmistamaan, että käyttäjä on kuka hän väittää olevansa. Nämä tekijäluokat ovat [7]:

- Tietotekijät, joihin sisältyvät käyttäjän salasana, tunnuslause, henkilökohtainen tunnusnumero (pin-koodi) tai vastaus ennalta valittuun turvakysymykseen.
- Omistustekijät, joihin sisältyvät esineet, jotka käyttäjällä on hallussaan, kuten pankkikortti, kannettava tunniste, laitteisto- tai ohjelmistokertainen salasana tai matkapuhelin.
- Luontaistekijät, joihin sisältyvät biometriset tunnisteet, kuten kasvojen, sormenjäljen tai verkkokalvon tunnistus.

Käyttäjä voidaan todentaa monin eri tavoin kuten käyttämällä salasanaa, älykorttia tai biometrista tunnistautumista. Salasanat ovat jotain, joka on tiedossa vain käyttäjällä. Salasana on yleisin käytetty todennustyyppi ja samalla yksi haavoittuvimmista. Salasanojen tulisi olla riittävän satunnaisia estääkseen hyökkääjä arvaamasta niitä ja samalla salasanat eivät saisi olla liian vaikeita käyttäjän muistaa. Muita salasanan haavoittuvuuksia ovat: paljastuminen olan yli kurkkimalla, varastettavuus, jos salasana on kirjoitettu paperille, salasanan tietoinen jakaminen tai salasanan arvaaminen. [4]

Salasanaa on yleisesti käytetty sisäänkirjautumiseen tietokoneisiin, ja useimmissa käyttöjärjestelmissä on sisäänrakennettu salasanan todennus, koska se on helpoin ja halvin vaihtoehto valitessa autentikointitapaa. Turvallisempi tapa on käyttää aikasalasanoja, jotka ovat käytössä vain kerran ja muuttuvat dynaamisesti jokaisen käytön yhteydessä. Tämän tyyppistä salasanaa voidaan käyttää käyttäjän hallussa olevissa digitaalisissa laitteissa tai salasana on yksinkertaisesti tulostettu salasanalistalle paperille. [8]

Älylaitteeseen ladattavalla tunnistussovelluksella voi kirjautua ja tunnistautua esimerkiksi verkkopankkiin. Sovellukset käyttävät samaa laitteisto-tunnuskonseptia, mutta tunnistautuminen tehdään ohjelmiston avulla, joka asennetaan käyttäjän laitteelle. Käyttö on edullista, mutta on haavoittuvainen haittaohjelmille kuten kaikki ohjelmistot. [8]

Digitaaliset sertifikaatit ja allekirjoitukset perustuvat julkisen avaimen menetelmään PKI (Public Key Infrastructure). Digitaalinen varmenne tallentaa käyttäjän julkisen avaimen, joka jaetaan vertaiskäyttäjille, kun taas vain käyttäjällä on pääsy yksityiseen avaimeen, joka on suojattu tunnuslauseella. Julkisen ja yksityisen avaimen välillä on aina yksilöllinen matemaattinen korrelaatio. Avaimia käytetään suorittamaan täydentäviä toimintoja, kuten salaus ja salauksen purku tai allekirjoitusten varmentaminen ja luominen.
Yksityistä avainta käytetään sähköisen allekirjoituksen tekemiseen. Julkista avainta käytetään sähköisen allekirjoituksen tarkistamiseen. [5]

Älykortit kykenevät turvallisesti tallentamaan yksityisen avaimen ja sitä vastaavan digitaalisen varmenteen, joten sitä ei tallenneta mihinkään muuhun laitteeseen. Edistyneiden salausominaisuuksien vuoksi älykorttitodennus on turvallisempaa kuin salasanojen käyttö. Käyttämällä PIN-koodia älykortin kanssa suojaustasoa saadaan lisättyä. [8]

Biometrinen käyttäjän autentikointi on menetelmä, joka tunnistaa käyttäjän ja varmistaa hänen henkilöllisyytensä ainutlaatuisten fysiologisten piirteiden tai käyttäytymisominaisuuksien mittaamisen perusteella. Fysiologisia biometrisiä tietoja ovat sormenjäljet, kasvojentunnistus, iiriskannaus, käden geometria sekä verkkokalvon skannaus. Käyttäytymiseen liittyvä biometriaa ovat äänentunnistus, näppäinpainallukset sekä allekirjoitusten skannaukset. Biometriseen todennukseen vaaditaan, että käyttäjällä on pääsy erikoislaitteisiin, jotka voivat skannata sormenjäljet, verkkokalvon tai iiriksen. [9]

2.3 Autentikoinnin uhat ja turvallisuusnäkökohdat

Yksityisyyden suoja ja tietoturvauhat ovat ensisijaisia huolenaiheita käytettäessä digitaalista autentikointia. Autentikoinnin monimutkaistuessa, kun esimerkiksi käytetään useita autentikointitekijöitä tai suojattua yhteyttä tunnisteen ja tietokannan välillä, voi prosessi tuntua käyttäjän näkökulmasta aikaa tuhlaavalta. Tosiasiassa mikään turvajärjestelmä ei ole täysin varma. Lisäksi mitä hienostuneempi todennusjärjestelmä on, sitä suurempi on mahdollisuus häiriöiden esiintymiseen. Tässä kohdassa on kuvattu digitaalisen autentikoinnin mahdollisia uhkia esimerkkien avulla. [10]

- Väärän varmenteen valmistus tai muokkaus: Vaarantunut CSP (Cryptographic Service Provider) tai välityspalvelin vahvistaa hakijan henkilöllisyyden, jota ei ole todennettu oikein.
- Varkaus: fyysisen tunnisteen varkaus (laitteiston salauslaite tai matkapuhelin)
- Tunnisteen kopiointi: paperiin kirjoitetun tai sähköiseen tiedostoon tallennetun salasanan kopiointi, ohjelmiston PKI-varmenteen (yksityinen avain) kopiointi tai väärennetty biometrinen varmenne.
- Salakuuntelu: olan yli kurkkiminen, näppäinpainallusten tallennusohjelma sieppaa salasanan tai PIN-koodin tai yhteiskäytössä olevan salasanan kaappaus toiselta käyttäjältä.
- Tietojen kalastelu tai urkinta: henkilöiltä yritetään saada esimerkiksi massasähköpostien tai väärennettyjen www-sivujen välityksellä tärkeitä henkilökohtaisia tietoja kuten käyttäjätunnuksia, pankkitunnuksia, luottokorttitietoja tai henkilötietoja.
- Sosiaalinen vaikuttaminen: sisältää ihmisen käyttämät kyvyt ja työkalut, joiden avulla voidaan päästä käsiksi sellaiseen tietoon, mitä kohdehenkilö ei välttämättä halua vapaaehtoisesti antaa esimerkiksi pankkitunnusten tai salasanan kertominen, tai ulkopuolisilta rajatulle alueelle päästäminen.
- Salasanan arvaus: salasanan arvaamiseen tarkoitettu hyökkäys, joka koostuu kaikkien mahdollisten koodien, yhdistelmien tai salasanojen kokeilusta, kunnes oikea yhdistelmä löytyy.
- Päätelaitteen vaarannus: yritysverkkoon on tuotu käyttäjän tartuttama laite, joka toimittaa sivusuunnassa leviäviä haittaohjelmia tai käyttäjät huijataan haittaohjelmien lataamiseen ja asentamiseen väittämällä, että ne ovat virustorjunta-, levyn puhdistus- tai muu apuohjelma.

Edellä kuvattujen uhkien lieventämiseksi voidaan käyttää useita eri menetelmiä. Usean eri autentikointitekijän käyttö yhdessä voi vaikeuttaa hyökkäyksiä. Jos hyökkääjän täytyy sekä varastaa salauksen varmenne, että arvata muistiin tallennettu salasana, toimenpiteet molempien tekijöiden löytämiseksi saattavat olla liian työläitä. [11]

Fyysisiä turvamekanismeja voidaan käyttää varastetun varmenteen suojaamiseksi kopioinnilta. Fyysiset turvamekanismit voivat tarjota peukaloinnin eston, havaitsemisen ja reagoinnin. Pitkien salasanojen, joita ei esiinny yleisissä sanakirjoissa, käyttö pakottaa hyökkääjät kokeilemaan kaikkia mahdollisia arvoja. Järjestelmän ja verkon suojaustoimintoja voidaan käyttää estämään hyökkääjää pääsemästä järjestelmään tai asenta-

maan haittaohjelmia. Säännöllinen koulutus auttaa käyttäjiä ymmärtämään, milloin ja miten ilmoittaa riskitekijöistä tai epäilystä tai muuten tunnistaa käyttäytymismalleja, jotka voivat merkitä hyökkääjää, joka yrittää vaarantaa todennusprosessin. [10]

Lisäksi vältetään sellaisten varmenteiden käyttöä, jotka aiheuttavat kolmansien osapuolten, kuten asiakaspalvelun, sosiaalisen vaikuttamisen riskin. Käytetään varmenteita, joka lukittuvat useiden toistuvien epäonnistuneiden aktivointiyritysten jälkeen, jotka vaativat käyttäjän fyysisen toiminnan sekä pidetään ohjelmistopohjaiset avaimet rajoitetun käyttöoikeuden tallennustilassa. [10]

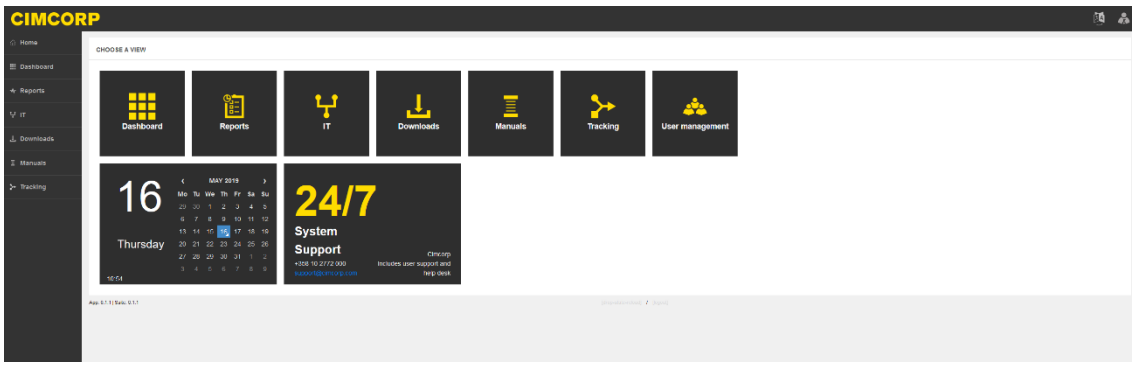
3. KÄYTTÖLIITTYMÄN AUTENTIKOINTI TUTKIMUSKYSYMYKSENÄ

Tässä luvussa esitellään diplomityön perustana oleva tutkimuskysymys. Cimcorp:in varastonhallintajärjestelmän käyttöliittymän autentikointi on perinteisesti tapahtunut käsittelemällä käyttäjien tunnistetiedot ohjelmakoodista käsin. Tunnistetiedot on tallennettu tietokantaan. Sisäänkirjautumisen toteuttaminen tietokantapohjaista autentikointia hyväksi käyttäen on ollut nopein tapa toteuttaa autentikointi ja hallinnoida suuria määriä tunnistetietoa.

Diplomityön tarkoituksena on tutkia, miten käyttäjän autentikointi voidaan toteuttaa ulkopuolista tunnistautumisjärjestelmää hyväksi käyttäen. Autentikoinnin perusperiaate eroaisi aiemmin käytössä olevasta tekniikasta, sillä käyttäjien tiedot tallennettaisiin järjestelmän ulkopuoliseen tietokantaan. Tunnistautuminen tapahtuisi muualla toisessa palvelussa olemassa olevasta järjestelmästä erillään. Tunnistautumiseen käytettävä palvelu palauttaisi vaadittavat autentikointitiedot kohdepalvelulle, joiden perusteella käyttäjä voitaisiin tunnistaa.

3.1 Hallintajärjestelmien käyttöliittymät

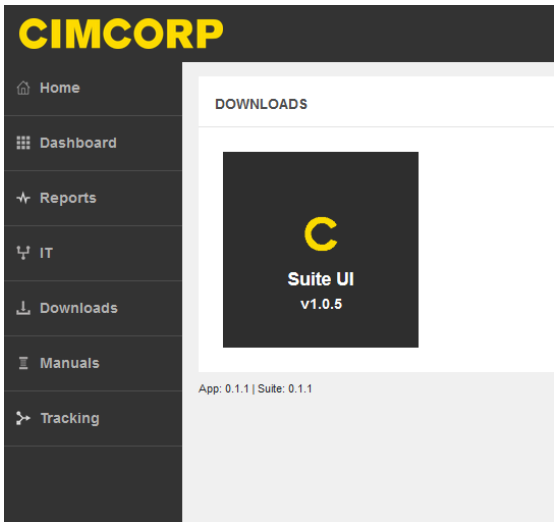
Cimcorp:in tarjoama hallinnan käyttöjärjestelmä verkkosovellus, johon kirjaudutaan soveltuvalla web-selaimella. Käyttöliittymäsovelluksella voidaan esimerkiksi konfiguroida järjestelmän eri osia, lukea käyttöohjeita, ladata hallintaan tarvittavia tiedostoja, seurata järjestelmän nykyistä tilaa ja saada raportteja järjestelmän historiatietokannasta. Käyttöliittymä on toteutettu REST- ja WebSocket-rajapinnoilla ja palvelinpää (backend) on Java EE-pohjainen. Web-sovelluksen aloitusnäkymä on esitetty kuvassa 1.



Kuva 1 Cimcorp hallinnan käyttöjärjestelmän aloitussivu

Käyttöliittymä on suunniteltu mukautuvaksi, joten sitä on mahdollista käyttää myös mobiililaitteiden kanssa. Mukautuvassa suunnittelussa verkkosivusto näyttää saman sisällön kaikille laitteille, mutta sisältö on muotoiltu eri tavalla käytettävissä olevan tilan mukaan. Kannettavaa laitetta on helpompi kuljettaa mukana liikuttaessa tehdasalueella.

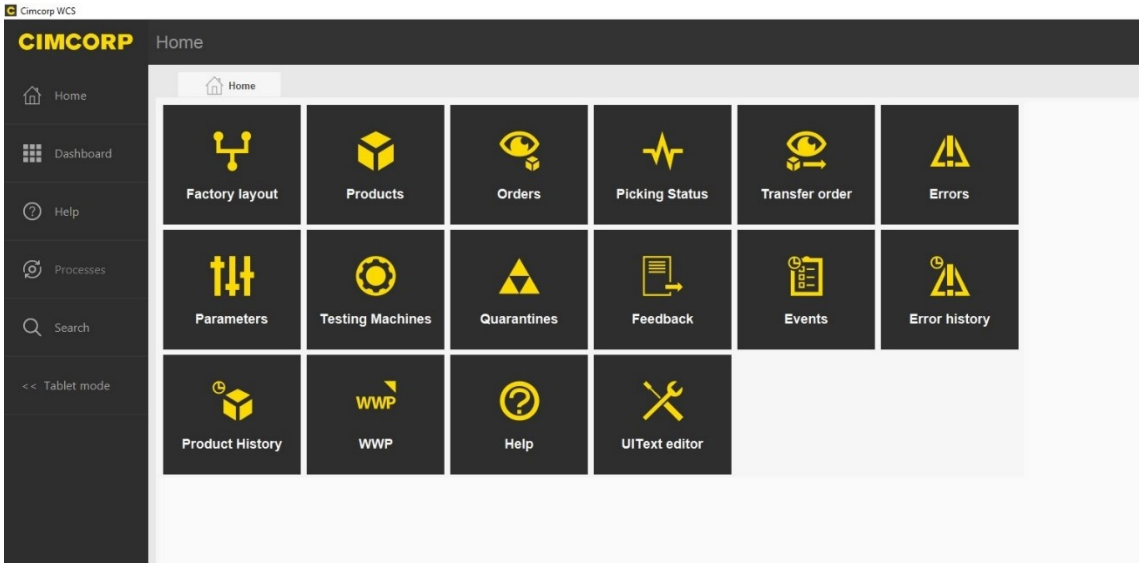
Cimcorp-järjestelmä sisältää Java FX –pohjaisen työpöytäsovelluksen muiden automaatiojärjestelmän toimintojen käyttämiseen. Käyttäjä voi asentaa sovelluksen koneelleen web-sovelluksen sivulta. Asennus tehdään normaalisti vain kerran ohjelman käyttöönoton yhteydessä. Ohjelman asennus aloitetaan asennuspaketin latauksella napsauttamalla ohjelman painiketta web-sovelluksesta. Asennusohjelma asentaa ohjelman tietokoneelle ja luo kuvakkeen työpöydälle. Varastohallintasovelluksen asennussivu on esitetty kuvassa 2.



Kuva 2 Työpöytäsovelluksen asennussivu

Cimcorp:in varastonhallintajärjestelmän käyttöliittymä on tarkoitettu automaatiojärjestelmän eri osien hallintaan. Käyttöliittymän kautta ohjataan varaston tuotekeräilyä ja materiaalivirtoja sekä hallinnoidaan valmistustietoja sekä tuotteiden jäljitettävyyttä. Käyttöliittymän ominaisuuksia ovat siirrettävyys ja yhdestä paikasta tapahtuva SPOC-ohjaus (Single Point of Control) varastonhallinnalle ja laitteille kuten roboteille ja kuljettimille.

Varastonhallintajärjestelmä on tietokannan ohjaama laite- ja tilaustenkäsittelyjärjestelmä. Varastonhallintajärjestelmän käyttöliittymä aloitussivu on esitetty kuvassa 3. Aloitussivun valikon ikkunat voidaan avata omaksi välilehdekseen, josta voidaan nähdä toiminnot, jotka on jo käynnistetty.



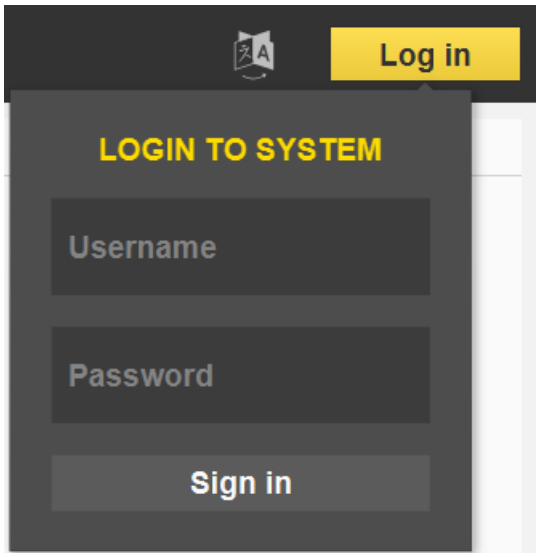
Kuva 3: Cimcorp varastonhallintakäyttöliittymän aloitusnäkymä

Käyttöliittymä tukee myös kosketusnäyttöjä. Kosketusnäyttöjä käytetään raskaan teollisuuden parissa, missä perinteiset ohjauslaitteet ovat epäkäytännöllisiä. Painikkeet ovat isoja, joten niitä on helppo käyttää myös kosketusnäytöltä.

3.2 Käyttöliittymän sisäänkirjautuminen

Järjestelmän käyttäjä eli operaattori voi tarkastella ja valvoa järjestelmää kirjautumatta sisään. Sisäänkirjautuminen on tehtävä, kun jotain on tarpeen muuttaa. Käyttäjälle asetettu rooli määrittelee käyttäjälle sallitut näkymät ja tehtävät. Järjestelmään on yleensä luotu ennalta määrättyjä rooleja, joille on ennalta määritelty käyttöoikeustaso.

Operaattori voi kirjautua sisään missä tahansa järjestelmässä painamalla painiketta käyttöliittymäsovelluksen oikeassa yläkulmassa. Kuvassa 4 esitetty sisäänkirjautumisen valintaikkuna avautuu. Käyttäjältä kysytään käyttäjätunnusta ja salasanaa.



Kuva 4 Sisäänkirjautumisikkuna

Koska käyttöliittymää voidaan käyttää myös esimerkiksi trukkipäätteeltä, on sisäänkirjautuminen hitaampaa, kun käyttäjätiedot syötetään kirjain kerrallaan. Työntekijöiden sisäänkirjautuminen ja kirjautuminen ulos tunnisteella olisi nopeampaa ja helpompaa. Tunnisteen käytön myötä riski jaetuista salasanoista tai tileistä poistuisi. Tunnisteen käyttö tarjoaisi asiakkaalle tarkastusketjun sekä mahdollisuuden hyödyntää jo olemassa olevia tunnisteita esimerkiksi henkilökortteja.

Diplomityön tarkoituksena oli tutkia, miten käyttäjän autentikointi voidaan toteuttaa ulkopuolista tunnistautumisjärjestelmää hyväksi käyttäen. Tutkimuksen kohteena olevan toteutuksen toimintaperiaatteena olisi saattaa järjestelmään kirjautuneen käyttäjän syöttämä RFID-tunniste web-palvelimen välityksellä LDAP-hakemistopalvelimelle. Järjestelmään kirjautuminen tapahtuisi käyttöliittymäsovelluksen sekä RFID-tunnisteen ja -lukijan avulla. Käyttäjä tunnistettaisiin LDAP-hakemistopalvelimelta sisäänkirjautumissivulle syötetyn käyttäjätunnuksen ja salasanan yhdistelmällä tai RFID-lukijaan syötetyn kortin sarjanumeron perusteella.

Sisäänkirjautumisen yhteydessä LDAP-palvelimelta haettujen, käyttäjää koskevien attribuuttien arvot määräisivät käyttäjän roolin ja ryhmän. Käyttäjälle asetetusta roolista riippuen käyttöliittymän aloitusnäkymän sisältö ja käyttäjän oikeudet voitaisiin mukauttaa rooliryhmän mukaiseksi.

Mikäli käyttäjätunnus, salasana tai kortin sarjanumero ei täsmäisi LDAP-hakemistopalvelimen tietoihin tai todennuspalvelimeen (LDAP-palvelin) ei saada yhteyttä, niin sisäänkirjautumissivulle ilmestyisi asiaan liittyvä virheviesti.

4. RFID TEKNOLOGIA

RFID on lyhenne sanoista Radio Frequency Identification eli radiotaajuinen etätunnistus. Tämä tekniikka käyttää sähkömagneettisia kenttiä etälukuun ja -tallentamiseen RFID-tunnisteilta. RFID-tunnisteet lähettävät ja vastaanottavat radiotaajuisia kyselyitä antennin avulla RFID-lähetin-vastaanottimelta. RFID on vaihtoehto viivakoodeille suuremman lukuetäisyyden ja kestävyyden vuoksi. [12]

4.1 Arkkitehtuuri

RFID-järjestelmä koostuu yleensä kolmesta komponentista: tunniste, lukija ja palvelin. Tyypillinen arkkitehtuuri on esitetty kuvassa 5. Tunniste on integroitu piiri kytkettynä antenniin. Tunnisteella voi olla joko oma virtalähde tai lukijan antama. Aktiivisessa tunnisteessa on mukana oma virtalähde (paristo tai akku). Passiivisen tunnisteen tarvitsema käyttöjännite siirretään tunnisteeseen lukijalaitteelta lukutapahtuman yhteydessä. [13]

Passiivinen tunniste sisältää antennin, jota käytetään kahteen tarkoitukseen: energian keräämiseksi lukijasignaalista sekä kommunikointiin lukijan kanssa. Tunnisteen vastaanottama energian määrä riippuu monista tekijöistä, mutta tärkeimmät tekijät ovat lukijan ja tunnisteen välinen etäisyys, lukijalähettimen teho ja RFID-tunnisteantennien tehokkuus. Aktiivitunnisteen luentaetäisyys on pitempi ja hankintahinta korkeampi. [12]

Lukuetäisyys vaihtelee muutamasta senttimetristä useisiin metreihin. Tyypillisesti ympyräpolarisoiduilla antenneilla ei saavuteta yhtä suurta etäisyyttä kuin lineaarisesti polarisoiduilla antenneilla. Ympyrän muotoisesti polarisoidun antennin käyttö on suosoiteltavaa silloin, kun lukijan/tunnisteen suunta vaihtelee. Käytännössä lineaarisesti polarisoituja antenneja käytetään, kun vaaditaan suurin etäisyys ja lukijan/tunnisteen suunta on stabiili. Tunnisteen lukemaväli on lukija-antennin ja tunnisteen välinen maksimietäisyys, jolla lukija pystyy dekoodaamaan tunnisteen vastauksia, kun tunnisteantenni on suotuisasti orientoitunut lukija-antennin signaalin etenemisalueella. Tunnisteita parannetaan jatkuvasti, jotta ne voidaan lukea tehokkaammin ja suuremmalla etäisyydellä. Paradoksaalisesti tämä voi joskus olla ongelma, kun viereinen lukija lukee RFID-tunnistetta, aiheuttaen väärän positiivisen luennan. [12]

Tunnisteen muisti voi vaihdella sadasta bitistä muutamaan kilotavuun. Osa tunnisteista suorittaa vain logiikkaoperaatioita, kun taas osa laskee esimerkiksi julkisen avaimen salauksen. Tunnisteiden tietojen suojaamiseen on käytettävissä useita teknisiä tapoja. Tunnistemuistin käyttöoikeus voi rajoittaa tunnistekomentojen käyttöä ja suojata tunnisteen muistiin tallennettuja tietoja. Tunnisteessa on minimissään yksilöivä koodi, joka voi olla valmistajan sarjanumero tai EPC-koodi (Electronic Product Code). Suuremman muistikapasiteetin tunnisteiden tiedot voidaan uudelleen kirjoittaa sisältämään erilaista informaatiota. Monet tunnisteet tukevat salasanalla suojattua lukitusominaisuutta luku- ja kirjoitusoperaatioille. Joissakin RFID-tekniikoissa lukitusominaisuus on pysyvä ja toisissa palautuva. Muisti on joko luku- ja kirjoitussuojattu tai vain kirjoitussuojattu. Lukitusominaisuus estää luvattomia käyttäjiä lukemasta/käyttämästä tunnisteiden tietoja. [12]

Tunnisteeseen tallennetut tiedot voidaan salata ennen kuin ne kirjoitetaan tunnisteeseen. Tämä suojaus ei edellytä, että tunniste salaa tai purkaa tietoja. Sen sijaan salauksen suorittaa joko lukija tai muu yrityksen järjestelmän ohjelmisto. Tunnisteen toiminnot voidaan myös poistaa pysyvästi etäkomennon avulla. Komento on suojattu 32-bittisellä salasanalla, joka eroaa käyttösalasanasta. [12]

Lukija on lähetin-vastaanotin. Lukija kommunikoi tunnisteen kanssa, kun tunniste on lukijan sähkömagneettisessa kentässä. Se voi myös kommunikoida muiden lukijoiden tai taustajärjestelmän kanssa esimerkiksi langattoman verkon kautta. Lukija on yleensä tehokkaampi kuin tunniste: sen laskentakapasiteettia voidaan verrata pieneen tietokoneeseen. [13]

Palvelin sisältää tietokannan, joka puolestaan sisältää järjestelmän jokaiseen tunnisteeseen ja lukijaan liittyvät tiedot. Palvelin voi olla myös eräänlainen kytkin, joka välittää vain lukijoiden välistä viestintää. Palvelin voi kommunikoida vain lukijoiden kanssa. Palvelinta ei välttämättä tarvita, jos järjestelmä koostuu itsenäisestä lukijasta, jolla voi olla myös palvelimen rooli. Lukija lähettää radiotaajuuden kantoaaltosignaalin, joka heijastuu RFID-tunnisteella. Lukija muuntaa RFID-tunnisteelta saamansa viestin digitaaliseen muotoon, joka välitetään palvelimelle käsiteltäväksi. [13]

Kuva 5 RFID arkkitehtuuri

RFID-tekniikka toimii pääasiassa viidellä taajuuskaistalla standardin ISO/IEC 18000 mukaisesti. [14] Tunnisteen taajuusalueen valinta riippuu monista perusteista, kuten antennin koosta, taajuuskaistoja koskevista määräyksistä maassa, jossa RFID-järjestelmä on käytössä, tai käytön helppoudesta ja sen seurauksena tuotantokustannuksista.

4.2 Sovelluskohteet

Teollisuudessa on käytössä monia RFID-pohjaisia sovelluksia. Sovellukset voidaan jakaa kolmeen luokkaan: käyttöoikeuksien hallinta, seurannan ja tuotannon hallinta ja turvasovellukset. [13] Tässä kohdassa esitellään esimerkkejä näiltä kolme alueelta.

Käyttöoikeuksien hallinnassa RFID-teknologian tärkeimpiä sovelluskohteita ovat maksujärjestelmät, lipunmyynti (hiihtokeskusten kulunvalvonta), autojen käynnistyksen- ja varkaudenestojärjestelmät, tiemaksut ja julkinen liikenne. Lipunmyyntiautomaatit aiheuttavat kuljetusyrityksille kustannuksia kunnossapidon ja korjauksien (seteleiden ja kolikoiden täyttäminen, vikojen korjaukset, ilkivallan aiheuttamat vahingot) muodossa. Alennukset voidaan laskea vain kalliiden satunnaislaskelmien perusteella, mikä johtaa laskelmien epätarkkuuteen. [15]

Vaikka RFID-järjestelmän hankintakustannukset ovat edelleen korkeammat kuin esimerkiksi perinteisen lippujärjestelmän, sijoitus voi maksaa itsensä takaisin lyhyessä ajassa. Käteistä ei enää tarvita, tunnisteet voidaan ladata suurilla summilla, tunniste pysyy voimassa, vaikka hintoja muutetaan, myyntiautomaattien ja lipunvalvojien käyttö- ja ylläpitokustannukset alenevat. Onnistunut hyökkäys tällaiseen järjestelmään voi kuitenkin

merkitä yritykselle laaja-alaisia taloudellisia vaurioita, kun esimerkiksi myydään väärennettyjä tunnisteita. Tällaisissa sovelluksissa tunniste, jolla on korkeatasoinen todennus- ja salausmekanismi, on välttämätön. [15]

Elektronisia kulunvalvontajärjestelmiä käytetään tarkistamaan henkilöiden pääsyvaltuudet rakennuksiin (liike- tai tapahtumapaikkoihin) tai yksittäisiin huoneisiin. Online-järjestelmässä suuri määrä henkilöiden pääsyvaltuutuksia on tarkastettava vain muutamalla sisäänkäynnillä kuten toimistorakennusten ja liiketilojen pääsisäänkäyntien yhteydessä. Tämän tyyppisessä järjestelmässä kaikki päätelaitteet on kytketty keskustietokoneeseen verkon avulla. Offline-järjestelmät ovat yleisiä tilanteissa, joissa on monta yksittäistä huonetta, joihin vain harvalla pääsy, varustetaan elektronisella kulunvalvontajärjestelmällä. Tunniste ohjelmoidaan keskusasemalle, esimerkiksi hotellin vastaanotossa vieraan saapuessa. Valtuutettujen huoneiden lisäksi tunniste voidaan ohjelmoida myös tiettyyn voimassaoloaikaan, jotta esimerkiksi hotelliavaimet mitätöidään automaattisesti vieraan lähtöpäivänä. [15]

Seurannan ja tuotannon hallinnassa käyttökohteita ovat lemmikkieläinten tunnistesirut, kirjastot ja teollisuuden toimitusketjun seuranta. Ihmisten jäljittäminen on mahdollista, jos he kantavat tai käyttävät esineitä, joissa on RFID-tunniste. Esimerkiksi huvipuistoissa voidaan tunnisteita käyttää lapsien löytämiseksi vanhemmilleen. Tunnistetta käytetään hiihtokeskuksissa auttamaan ystäviä löytämään toisiaan, sairaaloissa potilaiden seurantaan ja vankiloissa vankien seurantaan koko laitoksen alueella. Seuranta on mahdollista keräämällä tai käsittelemällä sijainti- ja aikatietoja ja se voidaan suorittaa joko tietokantaan tallennetuilla tiedoilla jälkikäteen tai reaaliajassa. [16]

RFID:tä käytetään nykyään teollisuudessa viivakoodin sijaan, koska viivakoodin käyttöikä on verrattain lyhyt ja RFID ei vaadi suoraa yhteyttä lukijan ja tunnisteen välille. Nykyaikaisilla tuotantolinjoilla tuotteiden laatua testataan useilla testiasemilla. Kun tuotetta tarkastetaan tuotantoprosessin lopussa, on oltava mahdollista yksiselitteisesti osoittaa aiemmin kerätyt laatutiedot tietylle tuotteelle. Tuotteen mukana kulkevilla kirjoitettavilla tunnisteilla tämä on helppo saavuttaa, koska kaikki tuotantoprosessin aikana saadut tiedot kulkevat tuotteen mukana. Tarvittaessa tuote voidaan vetää pois tuotantoprosessista menettämättä tietoja. Jos tuote palautetaan myöhemmin prosessiin, se voi jatkua ilman ongelmia tai vikoja. [15]

Turvasovelluksiin kuuluu esimerkiksi sähköinen passi, johon voidaan upottaa tunniste, johon on tallennettu tiedot passinhaltijasta, kuten syntymäaika, sukupuoli, passin haltijan

nimi sekä haltijan kuva ja sormenjäljet. Tunnisteessa olevien tietojen eheys varmistetaan erilaisilla mekanismeilla ja datanluku on suojattu todennusprotokollalla. [13]

4.3 RFID-järjestelmän suojaus

Järjestelmän hankkimiseen ja toteuttamiseen liittyvät kustannukset voivat muodosta käyttöönotolle huomattavasti suuremman esteen kuin muille todennusmenetelmille. Lisäksi monilla organisaatioilla on jo olemassa kortti- ja lukulaitteita. Näiden olemassa olevien investointien kopiointi ja korvaaminen merkitsevät huomattavia kustannuksia, mikä voi estää muutokset, huolimatta tunnisteiden tarjoamista parannetuista turvaominaisuuksista. Vaikka tunnisteet mainitaan usein niiden turvallisuuden vuoksi, tietyt turvallisuushaitat ovat edelleen olemassa. Tunnisteet eivät auta tilanteissa, joissa verkkohyökkäykset johtuvat suojaamattomasta ohjelmistosta tai käyttäjän huijaamisesta alkuperäisen kirjautumisen jälkeen. [16]

Tunnisteiden ja lukijoiden hyötynä on niiden yksinkertainen fyysinen rakenne. Laitteiston suljettua ympäristöä ei voi manipuloida eikä rikkoa tahattomasti. Järjestelmä on immuuni ohjelmistokonflikteille, version noudattamiselle sekä muille ongelmille, jotka voivat vaikuttaa ohjelmistoalustaan. Yksi tunniste voi palvella useita tarkoituksia, jolloin käyttäjän ei tarvitse kuljettaa mukanaan useita tunnisteita. Samaa tunnistetta voidaan käyttää esimerkiksi rakennusten sisäänpääsyyn, turvalliseen tietokone- ja verkkoon pääsyyn sekä käyttäjätunnuksena (työntekijä tai vierailija). RFID-järjestelmät ovat immuuneja pölylle, kosteudelle, öljyille, jäähdytysnesteille, kaasuille, korkeille lämpötiloille ja vastaaville ongelmille, joita voi esiintyä tuotantoympäristössä. [15]

RFID-tunnisteisiin, lukijoihin sekä laitteiden väliseen viestintään liittyy suuri joukko mahdollisia riskejä, jotka liittyvät kolmeen turvallisuuden osa-alueeseen: saatavuus, eheys ja luottamuksellisuus. Esimerkkejä ovat palvelun epääminen, häiritseminen, kloonaaminen ja salakuuntelu. Tutkimuksissa on löydetty iso joukko haavoittuvia RFID-tuotteita ja -ohjelmistoja. RFID-tietoturvan varmistaminen vaatii yhdistelmää teknisiä ja ei-teknisiä keinoja riskien estämiseksi ja vähentämiseksi. [16]

RFID-järjestelmän käyttäjät on koulutettava tunnisteiden käyttöön. Tunnisteet voivat kadota, ne voidaan varastaa tai jakaa. Tunniste on pidettävä käden ulottuvilla, eivätkä ne ole kovin kestäviä ja ne voidaan helposti rikkoa. Käyttösääntöjen tulee olla yhdenmukaisia tai integroituja organisaation tietosuojakäytäntöön, joka käsittelee henkilökohtaisten tietojen tallentamista ja jakamista. Tietoturvakäytännöt vähentävät RFID-tekniikoiden

käyttöön liittyviä liiketoimintariskejä. Käytännöt tarjoavat vaatimuksia ja ohjeita henkilöille, jotka suunnittelevat, toteuttavat, käyttävät ja ylläpitävät RFID-järjestelmiä. Käytäntöjen olemassaolo ei kuitenkaan takaa, että käytäntöä noudatetaan. [17]

Yksityisyyden suojaa koskevat ongelmat ovat riski sekä yksittäisille henkilöille että organisaatioille. RFID-järjestelmät, jotka keräävät näkymättömästi tunnistettuihin tai tunnistettavissa oleviin henkilöihin liittyviä tietoja, herättävät tietosuojakysymyksiä, joita pidetään haasteena tekniikan käyttöönotolle. RFID-tekniikka saattaa paljastaa kolmansille osapuolille tietoja tunnisteiden kautta henkilöiden tietämättä. Tämä skenaario edellyttää lukijoiden läsnäoloa tunnisteiden ympäristössä ja kolmannen osapuolen kykyä muuntaa esineiden tunnistetiedot merkityksellisiksi tiedoiksi. [16]

Koska RFID suunniteltiin kohteiden nopeaa tunnistamista varten, tekniikka ei itsessään tarjoa keinoja tunnisteiden ja lukijoiden todentamiseksi. Tunnisteet luovuttavat tietonsa automaattisesti jokaiselle lukijalle. [18] RFID-tunnisteiden lisääntyvä käyttö esimerkiksi yrityksen kulkukorteissa voi aiheuttaa tietoturvariskejä. Sopiva radiotaajuus aiheuttaa sen, että kortin RFID-siru "vuotaa" tietoja kenelle tahansa, joka aktivoi sen. [19] Sen sijaan, että arkaluontoista tietoa tallennetaan tunnisteisiin, tiedot voidaan tallentaa suojattuun yrityksen alajärjestelmään ja hakea tunnisteen yksilöivällä tunnisteella. Täten yrityksen ulkopoliset tahot eivät voi saada tietoja tunnisteesta skannauksen tai salakuuntelun avulla. Tietojen salaus ja pääsynhallinta suoritetaan usein kustannustehokkaammin yrityksen omassa tietojärjestelmässä. [17]

Monet RFID-tuotteet tukevat kuitenkin vain murto-osaa mahdollisista suojamekanismeista. Erityisesti tunnisteiden laskentaominaisuudet ovat hyvin rajalliset. Useimmat tunnisteet eivät tue todentamista, pääsynhallintaa tai salausmenetelmiä, joita yleisesti käytetään muissa yrityksen IT-järjestelmissä. RFID-standardit määrittelevät suojausominaisuudet, mukaan lukien salasanat, joilla suojataan pääsy tiettyihin tunnistekomentoihin ja muistiin, mutta tarjottu tietoturvataso vaihtelee näiden standardien välillä. Myyjät tarjoavat myös patenttilaajennuksia standardipohjaiseen tekniikkaan, mutta ne eivät aina ole yhteensopivia järjestelmän muiden komponenttien kanssa. [17]

RFID-järjestelmien yleisimmät suojaustekniikat ovat salasanat, avaimellinen viestin hash-autentikointikoodi eli HMAC (Hash-based Message Authentication Code) ja digitaalinen allekirjoitus. Joissain tapauksissa todennustekniikan ensisijainen tavoite on estää tunnisteen luvaton lukeminen tai kirjoittaminen. Toisissa tapauksissa tavoitteena on havaita tunnisteiden kloonaus. Salaustekniikkaan perustuvat todennustekniikat tarjoavat

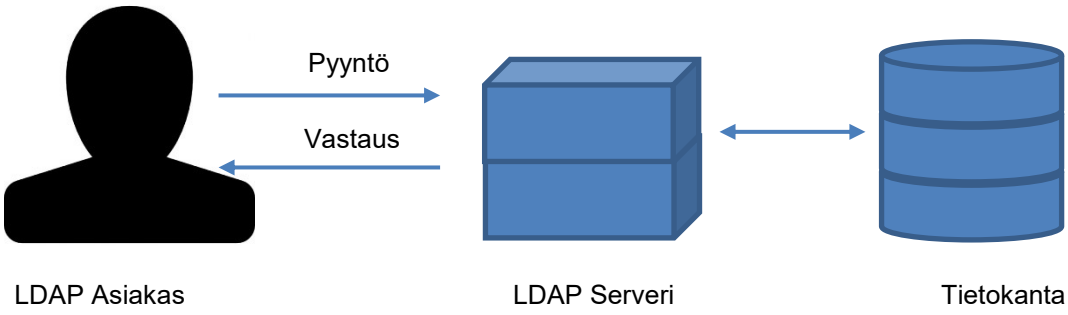
usein eheyspalveluita todennustapahtumaan sisältyvälle tiedolle eli tunkeutuja ei voi muuttaa tapahtuman tietoja ilman, että lukija tai tunniste tunnistaa muutoksen. [19]

Vaikka RFID-tekniikan käyttö lisääntyy useilla aloilla, niihin liittyviin tietoturva- ja yksityisyyskysymyksiin on perehdyttävä huolellisesti. Koska RFID-tunnisteita on olemassa erilaisia, ei ole olemassa yleistä tietoturvaratkaisua. Edulliset perustunnisteet eivät välttämättä sisällä salaustoimintoja, joita kalliimmat versiot sisältävät. Organisaatioiden, jotka haluavat käyttää RFID-tekniikkaa, on siis arvioitava kustannukset ja turvallisuusvaikutukset sekä ymmärrettävä eri RFID-tekniikoiden ja -ratkaisujen rajoitukset. RFID-järjestelmiin kohdistuvat riskit vaihtelevat huomattavasti käytetyn tekniikan mukaan, sovellusolosuhteiden ja skenaarioiden mukaan. Riskien arviointi- ja hallintasuunnitelma auttavat tunnistamaan tarpeen vahvistaa järjestelmän tiettyjä osia sellaisten heikkouksien kompensoimiseksi, joita ei voida suoraan käsitellä. [16]

5. LDAP

LDAP on lyhenne sanoista Lightweight Directory Access Protocol. Maailmanlaajuisen verkkopohjaisen hakemiston tarve johti siihen, että ITU (International Telecommunication Union) kehitti X.500-standardisarjan ja erityisesti X519:n, joka määritteli DAP:n (Directory Access Protocol), verkkopohjaisen hakemistopalvelun käyttöprotokollan. X.500-sarjan standardit ovat kuitenkin raskaita ja kuluttavat valtavasti resursseja. [20]

Raskaiden protokollien korvaamiseksi IETF (Internet Engineering Task Force) näki 90-luvun alussa tarpeen kevyemmälle protokollalle ja aloitti LDAP:in kehityksen. LDAP on suunniteltu tarjoamaan lähes yhtä paljon toimintoja kuin alkuperäinen X.519-standardi mutta halvemmalla ja TCP/IP-protokollaa käyttäen. LDAP:in toimintaperiaate on esitetty kuvassa 6. [21].



Kuva 6 Lightweight Directory Access Protocol

Vaikka LDAP-protokollaa käytetään edelleen X.500-hakemistopalvelun käyttämiseen yhdyskäytävien kautta, LDAP on nyt yleisemmin suoraan toteutettu X.500-palvelimissa. Standalone LDAP Daemon tai slapd (8) voidaan katsoa kevyeksi X.500-hakemistopalvelimeksi. Toisin sanoen se ei toteuta X.500: n DAP:aa eikä se tue koko X.500-mallia. Slapd (8) on LDAP-hakemistopalvelin, joka toimii useilla eri alustoilla. Sitä voidaan käyttää tarjoamaan hakemistopalvelua. Hakemisto voidaan liittää maailmanlaajuiseen LDAP-hakemistopalveluun tai suorittaa palvelu itse. Slapdin ominaisuuksia ovat [22]:

- LDAPv3: slapd toteuttaa Lightweight Directory Access -protokollan version 3.
- Yksinkertainen todennus ja suojauskerros: slapd tukee vahvoja autentikointi- ja tietoturvapalveluja SASL:n (Simple Authentication and Security Layer) avulla.

- TLS (Transport Layer Security): slapd tukee sertifikaattipohjaisia autentikointi- ja tietoturvapalveluja TLS:n avulla. [22]

5.1 Edut

LDAP:in käyttö on suositeltavaa, kun kohteena on tehtävä, joka vaatii nopeaa luku- ja kyselysuorituskykyä, mutta tietojen tallennus koskee vain pientä osaa merkinnöistä. Diplomityön kohteena oleva käyttäjän autentikointi on esimerkki halutusta toiminnasta. Ilman LDAP:n käyttöä käyttäjän on toimittava tietokannan kanssa vahvistaakseen käyttäjätunnuksen ja sen digitaalisen allekirjoituksen kirjautumisistuntoa varten. LDAP:in avulla koko organisaation tiedot voidaan yhdistää keskitettyyn arkistoon. Käyttäjän validointi voidaan eriyttää tietokantakyselyistä ja saavuttaa mahdollisesti suorituskyvyn parannuksia. LDAP toimii toisena tietokannan ulkopuolella olevana optimointikerroksena suorituskyvyn parantamiseksi, joka ei korvaa tietokantatoimintoja. [23]

LDAP tarjoaa standardoidun tiedonsiirtomenetelmän sekä paikallisille että etäyhteyksille. Näin ollen on mahdollista korvata LDAP-toteutus täysin ilman, että se vaikuttaa ulkoiseen rajapintaan. Koska LDAP käyttää standardoituja tiedonsiirtomenetelmiä, LDAP-asiakkaat ja palvelimet voidaan kehittää itsenäisesti. LDAP voi toimia myös useiden tietokantojen kanssa, mikä tarjoaa suuremman joustavuuden ympäristön kannalta parhaiten soveltuvien tietokantojen valitsemiseen. [21]

LDAP tarjoaa menetelmän, jonka avulla tietoja voidaan siirtää useisiin paikkoihin vaikuttamatta ulkoiseen pääsyyn kyseisiin tietoihin. Käyttämällä viittausmenetelmiä LDAP-tietoja voidaan siirtää vaihtoehtoisiin LDAP-palvelimiin muuttamalla vain toimintaparametreja. Täten on mahdollista rakentaa hajautettuja järjestelmiä, ehkä erillisistä itsenäisistä organisaatioista peräisin olevilla tiedoilla, samalla kun ne tarjoavat käyttäjilleen yhden, johdonmukaisen ja näkyvän kohteen tiedoille. LDAP:in etuja ovat näin ollen liiketoimintakriittisen tiedon hallinnan yhdenmukaisuus ja keskitetty tietoturva. [24]

LDAP-järjestelmät voidaan konfiguroida toimimaan replikoimalla dataa yhteen tai useampaan LDAP-palvelimeen tai -sovellukseen lisäämättä joko koodia tai muuttamalla ulkoista pääsyä näihin tietoihin. LDAP:in sisäänrakennettu replikointiominaisuus sallii yhden tai useamman hakemistorakenteen replikoinnin yhdeltä isännältä. LDAP:in ja transaktiotietokannan replikoinnin välillä on kuitenkin eroa. Kun päivitys suoritetaan LDAP-päähakemistossa, kaikkien orjien päivittäminen voi viedä jonkin aikaa eli isäntä ja

orjat voivat olla synkronoimattomia tietyn ajanjakson ajan. LDAP-järjestelmässä hakemistorakenteen synkronoinnin väliaikaista puuttumista pidetään merkityksettömänä. Toisaalta transaktiotietokannan tapauksessa jopa väliaikaista synkronoinnin puuttumista voidaan pitää katastrofaalisena. Tämä korostaa niiden tietojen ja niiden ominaisuuksien eroja, joita tulisi ylläpitää LDAP-yhteensopivassa hakemistossa verrattuna transaktiotietokantaan. [21]

5.2 AD ja OpenLDAP

LDAP:in kehityksen myötä syntyneet kaksi suurta hakemistopalvelua ovat AD (Microsoft Active Directory) ja OpenLDAP. Hakemistopalvelulla tarkoitetaan hakemistopalvelimen tarjoamaa palvelua, joka jakaa tietyillä edellytyksillä IP-verkon yli tähän tallennettuja tietoja. Tällaisia voivat esimerkiksi olla käyttäjän todentamiseen liittyvät tunniste- tai yhteystiedot. [24]

Microsoft AD:n (Active Directory) ja OpenLDAP:in ytimenä toimii LDAP-protokolla. Ajan myötä Microsoft on lisännyt Kerberosin AD:n protokollaksi ja hakemistopalvelu on näin sidottu tiukasti Windows-alustaan. Kerberos on verkon todennuspalvelu, joka kehitettiin parantamaan hajautettujen ympäristöjen turvallisuutta. Tämän myötä AD:sta on tullut suosittu valinta Windows-pohjaisissa verkoissa. Lyhennettä AD käytetään yleisesti hieman erheellisesti yleisnimityksenä hakemistopalveluille, vaikka se on ainoastaan yhden toimittajan vaihtoehto toteuttaa kyseinen palvelu. AD voi toimia LDAP-palvelimena, mutta se ei ole ainoastaan LDAP-protokollasta riippuvainen sovellus, vaan tarjoaa myös muita yhteysrajapintoja. [24]

AD DS (Active Directory Domain Service) käyttävää palvelinta kutsutaan toimialueen ohjaimeksi. Se todentaa ja valtuuttaa kaikki Windows-verkkotunnuksen verkon käyttäjät ja laitteet, määrittelee ja valvoo käyttöoikeuksia sekä asentaa tai päivittää ohjelmistoja. Esimerkiksi, kun käyttäjä kirjautuu laitteeseen Active Directory tarkistaa lähetetyn salasanan ja määrittää, onko käyttäjä järjestelmänvalvoja vai normaali käyttäjä. Lisäksi se sallii tietojen hallinnan ja tallentamisen, tarjoaa todentamis- ja valtuutusmekanismeja ja luo kehyksen muiden asiaan liittyvien palvelujen käyttöönottoon. [25]

OpenLDAP on vapaa, avoimen lähdekoodin toteutus. Sitä julkaistaan omalla lisenssillään nimeltä OpenLDAP Public License. [26] LDAP on alustasta riippumaton protokolla. Useat yleiset Linux-sovellukset sisältävät OpenLDAP-ohjelmiston LDAP-tukea varten.

Tavallisesti HTML-sivu tai sovellus vastaanottaa LDAP-pyynnön, dekoodaa sen ja lähettää sen sitten palvelinohjelmalle käsittelyä varten. Kun palvelinohjelma täyttää pyynnön, se palauttaa tuloksen sovellukselle, joka sitten lähettää tuloksen LDAP-asiakkaalle. [27]

OpenLDAP on käytössä tämän työn toteutuksessa. Palvelin ei vielä tue aivan kaikkia kaupallisten vaihtoehtojen kehittyneimpiä ominaisuuksia, mutta tarjoaa kuitenkin vakaan alustan moniin eri käyttötarkoituksiin.

5.3 LDAP mallit

LDAP määrittelee neljä mallia, jotka kuvaavat sen toimintaa, minkä tyyppisiä tietoja voidaan tallentaa LDAP-hakemistoihin ja mitä tiedoilla voidaan tehdä. Nämä neljä mallia ovat [28]:

- Tietomalli: määrittelee, millaisia tietoja voidaan tallentaa LDAP-hakemistoon.
- Nimeämismalli: määrittelee, kuinka LDAP-hakemistossa olevat tiedot voidaan järjestää ja miten niihin viitataan.
- Toimintamalli: määrittelee, mitä LDAP-hakemiston tiedoilla voidaan tehdä ja miten niitä voidaan käyttää ja päivittää.
- Suojausmalli: määrittelee, kuinka tiedot voidaan suojata LDAP-hakemistossa ja millaisia oikeuksia käyttäjät ja sovellukset tarvitsevat hakemiston käyttämiseen.

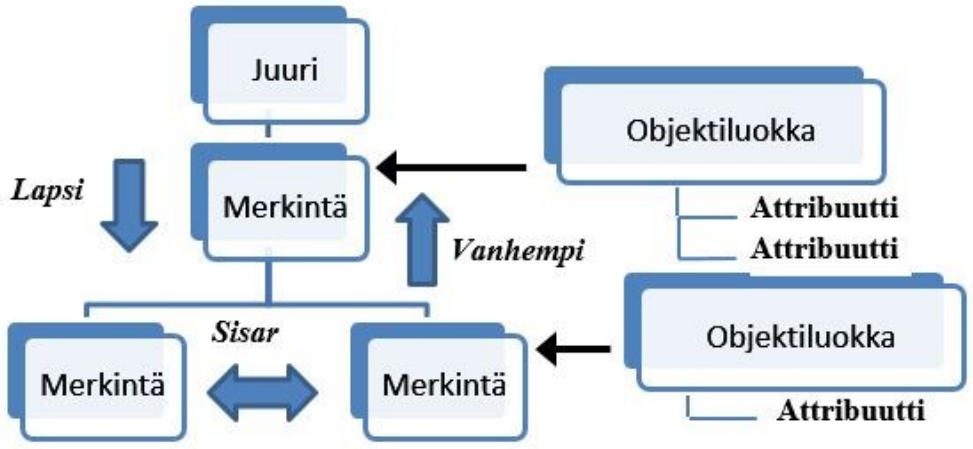
LDAP koostuu kaavioista (Schemas), objektiluokista ja attribuuteista. Kun LDAP:in puurakenteeseen lisätään merkintä, sen tiedot sisältyvät attribuutteihin, jotka on ryhmitelty objektiluokkiin, jotka on pakattu kaavioon. LDAP:in kaavio eli skeema on joukko sääntöjä, jotka määrittelevät käytetyt objektiluokat ja attribuutit. Kaaviota käyttämällä pystytään estämään väärien alaluokkien luominen objektiluokkaan sekä vähentämään duplikaattien määrää. Jokaisessa LDAP-hakemistossa on oletuskaavio, jota organisaatiot voivat mukauttaa tai laajentaa lisäämällä siihen elementtejä. [29]

Kun hakemistopuuhun lisätään uusi merkintä tai olemassa olevaa merkintää muutetaan, LDAP-hakemistopalvelimen tarjoaa mahdollisuuden valvoa järjestelmää, jotta LDAP-operaatioilla tehdyt hakemistomuutokset ovat kaavion mukaisia. Jos muutokset eivät ole skeeman määrittelyn mukaisia, palvelin palauttaa virheilmoituksen operaatiosta. [28]

LDAP:in monimutkaisuus ja toisaalta tehokkuus johtuvat siitä, että on olemassa paljon attribuutteja ja objektiluokkia, jotka ovat hajallaan eri skeemoissa. Helpointa on hyödyntää joitakin tunnettuja sovelluksia, jolloin käytössä on tunnettuja objektiluokkia ja määritteitä. Todellista perehtymistä aiheeseen vaatii selvittää, mitkä objektiluokat ja attribuutit ovat todella parhaita käsillä olevalle sovellukselle tai luoda vaihtoehtoisesti uusia. [21]

5.4 Tietomalli

Data esitetään LDAP-järjestelmässä objektien hierarkiana, joista kutakin kutsutaan tallennettavaksi tietueeksi tai merkinnäksi (entry). Tuloksena olevaa puurakennetta kutsutaan hakemistotiedon puuksi, DIT (Directory Information Tree). Puun yläosaa kutsutaan yleisesti juureksi (root). Puun esimerkkirakenne on esitetty kuvassa 7. [21]



Kuva 7 Hakemistotiedon puu, DIT

Jokaisella puun merkinnällä on yksi vanhemman merkintä (objekti) ja nolla tai useampi lapsen merkintä (objektit). Jokainen lapsen merkintä (kohde) on sen vanhemman muiden lasten merkintöjen sisar (sibling). Jokainen merkintä koostuu yhdestä tai useammasta objektiluokasta, joka sisältää nolla tai useampia määritteitä (attribuutti). Määritteillä on nimiä (ja joskus lyhenteitä tai aliaksia) ja ne sisältävät tyypillisesti tietoja. [21]

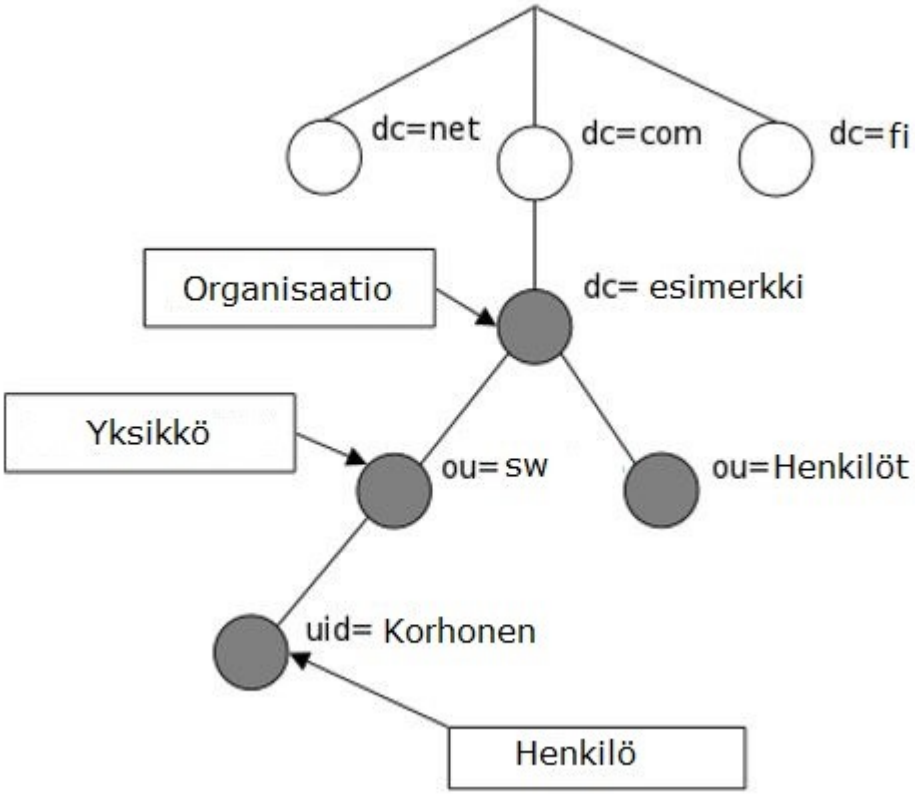
Objektiluokat toimivat attribuuttien säiliöinä ja jokaisella on yksilöllinen nimi. On olemassa ennalta määritettyjä objektiluokkia, joista kukin sisältää suuria määriä attribuutteja, jotka soveltuvat lähes kaikkiin yleisiin LDAP-toteutuksiin. Objektiluokilla on kolme muuta ominaisuutta: Objektiluokassa määritellään, onko attribuuttijäsen MUST (pakollinen olla läsnä) tai MAY (valinnainen olla läsnä). [21]

Kullakin objektiluokalla on tyyppi, joka voi olla STRUCTURAL, AUXILIAR tai ABSTRACT. Merkinnässä on oltava yksi ja vain yksi, STRUCTURAL objektiluokka, ja yksi tai useampi AUXILIARY objektiluokka. Objektiluokka voi olla osa hierarkiaa, jolloin se perii kaikki emo-objektiluokkansa ominaisuudet (mukaan lukien kaikki sen sisältämät attribuutit). [21]

5.5 Nimeämismalli

Jokainen LDAP:ssa käytetty nimi on ainutlaatuinen. Jokaisella objektiluokalla on yksilöllinen nimi. Myös kullakin määritteellä on yksikäsitteinen nimi DN (Distinguished Name) ja lyhenne tai alias, ja se sisältää yleensä tietoja. Attribuutit ovat yhden tai useamman objektiluokan jäseniä. Jokainen attribuutti määrittelee sen sisältämän tietotyypin eli syntaksin. Attribuutit voivat olla osa hierarkiaa, jolloin lapsiominaisuus perii kaikki vanhemman attribuutin ominaisuudet. [24]

Merkinnät järjestetään nimeämismallin mukaisesti hakemistoon edellisessä luvussa esitettyyn puumaiseen rakenteeseen. Hakemistopuun tietueiden järjestys perustuu määritteiden yksikäsitteisiin nimiin, jotka muodostetaan tietueen nimestä sekä hakemistopuussa edeltävien tietueiden nimistä. DN yksilöi merkinnän ja kuvaa sen sijainnin hakemistopuussa. Yksikäsitteinen nimi koostuu useammasta komponentista, joita kutsutaan nimellä RDN (Relative Distinguished Name). Jokainen RDN koostuu nimi-arvo-pareista. Jokaisessa RDN-nimessä on oltava vähintään yksi pari (attribuutin nimi, jota seuraa yhtäläinen merkki ja kyseisen attribuutin arvo). [28] Hakemistopuun nimeämisesimerkki on esitetty kuvassa 8.



Kuva 8 Hakemistopuun nimeämismalli [22]

Hakemistopuun esimerkissä puun rakenne kuvaa organisaation rakennetta. Juuren kautta on mahdollista päästä käsiksi puumallin jokaiseen osaan. Juuren alaisuudessa voi siten toimia useita rinnakkaisia järjestelmiä, jotka vähentävät hallinnan pullonkauloja ja ovat helposti skaalattavissa. Esimerkiksi henkilön vaihtaessa työtehtävää vain hänen yksikäsitteinen nimensä vaihtuu. [30]

Määritteet voivat olla valinnaisia tai pakollisia, kuten ASN.1-määrityksissä kuvataan sen objektiluokan osalta, jonka jäseniä ne ovat. Määrite voi olla valinnainen yhdessä objektiluokassa ja pakollinen toisessa. Objektiluokka määrittää tämän ominaisuuden. Määritteiden järjestys objektiluokassa ei ole merkittävä seikka. [17]

5.6 Tietojen lisäys rakenteeseen

Tietojen syöttö tapahtuu lisäämällä merkintöjä (niihin liittyvillä objektiluokilla ja attribuuteilla) puurakenteen juuresta alkaen ja etenemällä alas hierarkiassa. Siten vanhemman merkintä on aina lisättävä ennen lapsimerkintää. Kun DIT luodaan/täytetään, jokainen merkintä on yksilöitävissä vanhemman merkintään hierarkiassa.

Ainoa yksilöllinen elementti missä tahansa tietorakenteessa on data. Tietosisältö määritellään attribuutissa. Attribuutit voivat olla moniarvoisia eli ne voivat näkyä monta kertaa merkinnässä tai objektiluokassa, joissa on erilainen tietosisältö. Yksilöllisyyden saavuttamiseksi on tunnistettava sekä attribuutti että sen sisältämät tiedot. Tämä tehdään käyttämällä attribuutti-nimi = arvo -muotoa, jota kutsutaan LDAP-terminologiassa attribuuttiarvon määritykseksi, AVA (Attribute Value Assertion).
Merkintöjen lisääminen voidaan tehdä monin eri tavoin, joista yksi on käyttää LDIF-tiedostoja (LDAP Data Interchange Files). LDIF-tiedostot ovat tekstitiedostoja, jotka kuvaavat puuhierarkiaa ja jokaiselle attribuutille lisättävää tietoa. [21]

Seuraavassa on esitetty yksinkertainen esimerkki LDIF-tiedostosta, joka muodostaa root DN: n (dc = cimcorp, dc = com) ja lisää kolme lapsimerkintää people-merkinnän alle.

```
dn: dc=cimcorp,dc=com
dc: cimcorp
description: Esimerkki yritys
objectClass: dcObject
objectClass: organization
o: Cimcorp, Oy.

## Ensimmäisen tason hierarkia - työntekijät (people)
dn: ou=people, dc=cimcorp,dc=com
ou: people
description: Yrityksen kaikki työntekijät
objectClass: organizationalUnit

## Toisen tason hierarkia - työntekijän tiedot (people entries)
dn: cn=Esko Esimerkki,ou=people,dc=cimcorp,dc=com
objectclass: inetOrgPerson
cn: Esko Esimerkki
cn: Esko
sn: Esimerkki
uid: eesim
mail: esko@cimcorp.com
mail: e.esimerkki@cimcorp.com
```

```
ou: software

## Toisen tason hierarkia - työntekijän tiedot (people entries)
dn: cn=Teppo Testaaja,ou=people,dc=cimcorp,dc=com
objectclass: inetOrgPerson
cn: Teppo Testaaja
cn: Teppo
sn: Testaaja
uid: ttest
mail: teppo@cimcorp.com
mail: t.testaaja@cimcorp.com
ou: testing

## Toisen tason hierarkia - työntekijän tiedot (people entries)
dn: cn=Aatu Asiakastuki,ou=people,dc=cimcorp,dc=com
objectclass: inetOrgPerson
cn: Aatu Asiakastuki
cn: Aatu
sn: Asiakastuki
uid: aasia
mail: aatut@cimcorp.com
mail: a.asiakastuki@cimcorp.com
ou: support
```

LDAP-merkintöjen lisääminen voidaan tehdä myös LDAP-asiakasohjelmalla kuten yleiskäyttöisellä LDAP-selaimella tai erikoisohjelmalla kuten phpLDAPadmin, LDAP Account Manager ja Futurice. LDAP-palvelinohjelmia on käsitelty tarkemmin kohdassa 6.3.

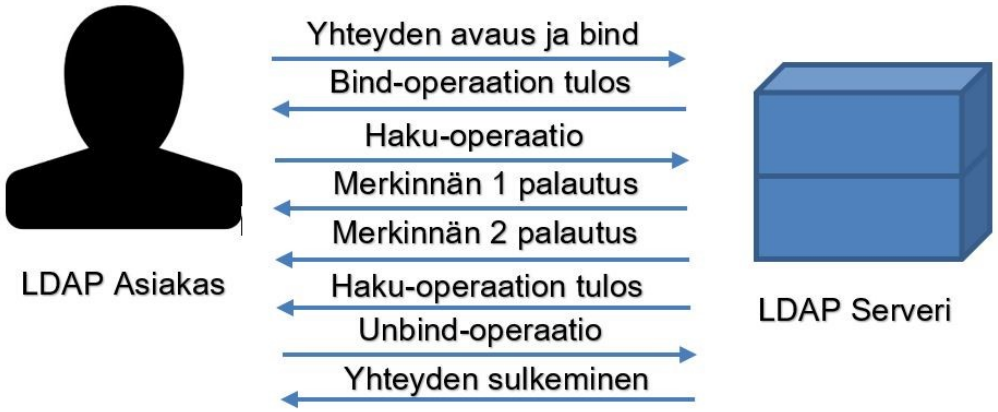
5.7 Toimintamalli

Toimintamalli määrittelee LDAP-protokollan toiminnan. Protokolla tarjoaa välineet hakemistopuun tietojen käyttämiseen. Kun tiedot on sijoitettu LDAP-hakemistoon, LDAP määrittelee yhdeksän erilaista toimintoa käyttäjien todentamiseksi, kun hakemistoa käy-

tetään, etsitään hakemistosta tai haetaan ja päivitetään tietoja hakemistossa. Pääsy toteutetaan todennusoperaatioilla (sidokset), kyselyoperaatioilla (haut ja luvut) ja päivitysoperaatioilla (kirjoitus). [28]

Todennusoperaatioita ovat bind ja unbind. Bind-operaatiolla LDAP-palvelin todentaa käyttäjän. Jos käyttäjä todennetaan onnistuneesti, LDAP-palvelin sallii asiakkaan pääsyn LDAP-palvelimelle kyseisen asiakkaan oikeuksien perusteella. Käyttäjä määrittää LDAP-palvelimen isäntänimen tai IP-osoitteen, jonka kannassa keskitetty osoitekirja sijaitsee. Lisäksi käyttäjä asettaa TCP/IP-porttinumeron, jonka kautta palvelin käsittelee tulevat LDAP-pyynnöt. Käyttäjä voi antaa käyttäjänimen ja salasanan todentaakseen palvelimen oikein. Kun käyttäjä lopettaa pyyntöjen tekemisen palvelimelle, se sulkee istunnon palvelimen kanssa unbind-operaatiolla. [31]

LDAP tarjoaa sekä luku-, haku-, että päivitysoperaatiot. Tämä mahdollistaa hakemistotietojen hallinnan ja kyselyn. Hakuoperaatio valitsee tiedot LDAP-puun määritellyltä alueelta valintaperusteiden perusteella. Jokaiselle vastaavalle merkinnälle voidaan palauttaa määritetty attribuuttijoukko (arvoilla tai ilman). Haetut merkinnät voivat kattaa yhden merkinnän, merkinnän välittömät lapset tai merkinnän koko alapuun. Alias-merkintöjä voidaan seurata automaattisesti haun aikana, ja asiakkaat voivat määrittää haun koon ja aikarajat. Päivitysoperaatioiden avulla lisätään, poistetaan sekä muokataan merkintöjä. [28] Esimerkki LDAP-asiakkaan ja serverin välisestä kommunikoinnista on esitetty kuvassa 9.



Kuva 9 LDAP-kommunikoinnin esimerkki

5.8 Suojausmalli

LDAP-palvelimet ovat osa organisaatioiden kriittistä rakennetta, jotka tallettavat henkilötietoja ja toimivat usein useiden sovellusten todennus- ja valtuutuslähteenä. LDAP-hakemistopalvelu tarjoaa joukon turvamekanismeja tallennettujen tietojen suojaamiseksi. Hakemistojen käyttäjien on ennen tietoihin pääsyä tunnistauduttava. LDAP:in eri versiot tukevat eri tyyppistä autentikointia. LDAP v2 määrittelee kolme eri tyyppistä autentikointia: nimetön (Anonymous), yksinkertainen (Simple) ja Kerberos v4. LDAP v3 tukee myös kahta eri autentikointi tyyppiä: Simple Authentication (RFC 4513) ja SASL (RFC 4422). LDAP v3 mahdollistaa uusien ominaisuuksien lisäämisen protokollaan laajennuksia käyttämällä ilman että protokollaa itsessään on muutettava. [32]

Bind-operaation Simple Authentication tarjoaa kolme eri todennusmekanismia: anonyymin, todentamattoman sekä nimen ja salasanan todennuksen. Anonyymissa todennuksessa ei käytetä nimeä tai salasanaa. Autentikointi sallitaan oletusarvoisesti. Todentamattomassa todennuksessa ainoastaan nimi on käytössä. [32]

Käytettävä autentikointimekanismi on oletuksena anonyymi, ellei autentikoinnin ympäristömuuttujia ole asetettu. Jos ympäristömuuttuja Context.SECURITY_AUTHENTICATION on asetettu arvoon "none", on autentikointimekanismi anonymous ja kaikki muut autentikoinnin ympäristömuuttuja sivuutetaan. Tämän autentikoinnin ollessa kyseessä käyttäjään suhtaudutaan nimettömänä. Tämä tarkoittaa, että palvelin ei tiedä tai ei välitä kuka käyttäjä on ja sallii käyttäjän pääsyn lukemaan tai päivittämään kaikkea tietoa, joka on konfiguroitu autentikoimattomalle käyttäjälle. [32]

Simple-autentikoinnin nimen ja salasanan todennus koostuu yksiselitteisen nimen, DN-nimen ja käyttäjän selkotekstisen salasanan lähettämisestä LDAP-serverille. Tällä mekanismilla on olemassa turvallisuusriski, koska salasana voidaan lukea verkosta käsin. Välttääkseen salasanan lukemisen voidaan käyttää simple-mekanismia salatun kanavan kautta (SSL tai TLS), jos LDAP-serveri tukee toimintaa. Koska LDAP:ia käytetään usein muiden palveluiden salasanojen vahvistamiseen, RFC 4513 mukaan palvelimen tulisi estää salasanojen käyttö, jos TLS ei ole käytössä. [33]

LDAD v3 käyttämä yksinkertainen todennus- ja suojauskerros (SASL) on liitettävä autentikointi. Tämä tarkoittaa, että LDAD asiakas ja serveri voidaan konfiguroida neuvottelemaan ja käyttämään mahdollisesti epätyypillisiä ja/tai räätälöityjä autentikointimekanismeja riippuen asiakkaan ja palvelimen vaatimasta suojaustasosta. [32]

SASL-mekanismeja on tällä hetkellä määritelty useita: [32]

- Anonymous (standardi RFC 2245)
- CRAM-MD5 (standardi RFC 2195)
- Digest-MD5 (standardi RFC 2831)
- External (standardi RFC 2222)
- Kerberos V4 (standardi RFC 2222)
- Kerberos V5 (standardi RFC 2222)
- SecurID (standardi RFC 2808)
- S/Key (standardi RFC 2222)

LDAP serverin tukemat SASL-mekanismit saadaan selville seuraavalla ohjelmalla:

```
// Luo alkuympäristö
DirContext ctx = new InitialDirContext();

// Lue tuetut SASL mekanismit
Attributes attrs = ctx.getAttributes(
  "ldap://localhost:389", new String[]{"supportedSASLMechanisms"}); [32]
```

Alla oleva tulos on saatu suorittamalla ohjelma palvelinta vastaan, joka tukee ulkoista SASL-mekanismia:

```
{supportedsaslmechanisms=supportedSASLMechanisms:
    EXTERNAL, GSSAPI, DIGEST-MD5} [32]
```

6. KÄYTTÄJÄTIETOJEN HALLINNAN TOTEUTUS

Tässä luvussa käsitellään diplomityön LDAP-palvelimen käyttäjätietojen hallinnan toteutus. LDAP-palvelimen asennuksen jälkeen palvelimelle on mahdollista lisätä käyttäjiä merkintöjen muodossa. Käyttäjien lisääminen on aikaa vievää, jos lisäys tapahtuu erillisen tiedoston avulla, joka sisältää kaikki alustetut LDAP-merkinnät, ja tiedosto tuodaan komentorivin kautta LDAP-palvelimelle. Nykyään on saatavilla monia kaupallisia ja ilmaisia LDAP-yhteensopivia graafisia sovelluksia ja apuohjelmia, joilla LDAP-palvelimen hallinta onnistuu vaivattomasta. Niiden tärkeimmät erot löytyvät järjestelmään sisällyttämisestä, laajuudesta, tuesta ja kustannuksista. Diplomityön yhtenä osa-alueena oli perehtyä muutamaan ohjelmistoon, joita voitaisiin hyödyntää Cimcorpin tietokannan ulkopuolisen hakemistopalvelun käytön kartoittamisessa.

6.1 LDAP-puun täyttö

LDAP rakenteessa on mahdollista käyttää useampia organisatorisia yksiköitä rinnakkain. Alla esitetyssä esimerkissä merkinnät sisältävät organisaation ihmiset, ryhmät ja roolit.

```
# People
dn: ou=people, dc=swsuite, dc=cimcorp, dc=com
objectclass: organizationalunit
ou: people
description: generic people branch

# Groups
dn: ou=groups, dc=swsuite, dc=cimcorp, dc=com
objectclass: organizationalunit
ou: groups
description: generic groups branch

# Roles
dn: ou=roles, dc=swsuite, dc=cimcorp, dc=com
objectclass: organizationalunit
ou: roles
```

```
description: generic roles branch
```

Kumpikin organisatorinen yksikkö ryhmät ja roolit voivat sisältää luettelon merkinnöistä, joissa käyttäjät ovat jäseninä jäsenattribuutin kautta.

```
# Create SW Dev Users group under groups
dn: cn=swdevgroup, ou=groups, dc= swsuite, dc= cimcorp, dc=com
objectclass: groupofnames
cn: swdevgroup
description: Finance team.
member: uid= virtanen, ou=people, dc=example, dc=com
member: uid= korhonen, ou=people, dc=example, dc=com

# Create Supervisor role under roles
dn: cn=supervisor, ou=roles, dc=swsuite, dc=cimcorp, dc=com
objectclass: groupofnames
cn: supervisor
description: Supervisor role (every member have 'supervisor' access)
member: uid=virtanen, ou=people, dc=swsuite, dc=cimcorp, dc=com
member: uid=korhonen, ou=people, dc=swsuite, dc=cimcorp, dc=com
```

Jos käyttöoikeussäännöissä on määritelty, että ryhmän jäsenet kuuluvat tiettyyn rooliryhmään, voidaan samaa merkintää käyttää sekä ryhmän että roolin jäsenyyksien säilyttämiseen. Käyttöoikeudet annetaan näin ollen ryhmän jäsenyydestä.

Jos käyttöoikeussäännöissä on määritelty, että tiettyyn ryhmään kuuluminen on ehto, mutta se ei riitä käyttöoikeuksien myöntämiseen tai se on riippumaton käyttöoikeussäännöistä, käytetään roolien jäsenyyksiä käyttöoikeuden myöntämiseen.

6.2 Varastonhallintajärjestelmän käyttäjäprofiilit

Tavallisesti varastonhallintajärjestelmässä on vain vähän erilaisia käyttäjäprofiileja. Kaikkien käyttäjien ei ole tarve tai oikeus tehdä kaikkea. Järjestelmässä on tavallisesti neljä tasoa. Tasot voivat olla käytössä varastonhallintaohjelmistossa tai tasoja voidaan olla käyttämättä. Käyttäjäprofiilien neljä eri tasoa on esitetty kuvassa 10.

Taso	Käyttäjäprofiili	Oikeudet	Käyttäjätason kuvaus
1	Prosessikoneen käyttäjä	Prosessikoneen paneeli Varastonhallinnan UI	Prosessikoneen käyttö ja ohjaus hallintapaneelin kautta. Laitteen käyttöliittymän käyttö.
2	Operaattori	Prosessikoneen paneeli Varastonhallinnan UI-näkymä	Prosessikoneen käyttö ja ohjaus hallintapaneelin kautta. Laitteen käyttöliittymän käyttö.
		Varastonhallinnan UI:n käyttö.	Varmistaa kaikkien laitteiden toiminnan. Varmistaa materiaalivirran sujuvuuden.
3	Valvoja	Prosessikoneen paneeli Varastonhallinnan UI-näkymä	Prosessikoneen käyttö ja ohjaus hallintapaneelin kautta. Laitteen käyttöliittymän käyttö.
		Varastonhallinnan UI:n käyttö.	Varmistaa kaikkien laitteiden toiminnan. Varmistaa materiaalivirran sujuvuuden.
		Varastonhallinnan UI:n käyttö	Varmistaa, että kaikki tilaukset kerätään. Varmistaa, että kaikilla prosessikoneilla on tehtäviä.
4	Pääkäyttäjä	Prosessikoneen paneeli Varastonhallinnan UI-näkymä	Prosessikoneen käyttö ja ohjaus hallintapaneelin kautta. Laitteen käyttöliittymän käyttö.
		Varastonhallinnan UI:n käyttö.	Varmistaa kaikkien laitteiden toiminnan. Varmistaa materiaalivirran sujuvuuden.

		Varastonhallinnan UI:n käyttö	Varmistaa, että kaikki tilaukset kerätään. Varmistaa, että kaikilla prosessikoneilla on tehtäviä.
		Käyttäjäoikeuksien hallinta	Ylläpitää käyttäjäasetuksia. Käynnistää / pysäyttää taustaprosessit tarvittaessa.

Kuva 10 Varastonhallintajärjestelmän käyttäjäprofiilit

Taso 1: Tason työtehtävä on yleensä helppo opettaa käyttäjälle. Työtehtävä on yleensä vain yksi osa järjestelmää, eikä koko järjestelmää ole tarve ymmärtää. Yleensä käyttäjä käsittelee yhden prosessikoneen toimintaa. Työtehtävä voi olla myös prosessin yksi toiminnallisuus, esimerkiksi yksiköiden rekisteröinti järjestelmään.

Taso 2: Tason työtehtävä on käsitellä poikkeukset, jotta materiaalivirta kulkisi sujuvasti. Operaattorin on ymmärrettävä järjestelmän materiaalivirtaus sekä laitteiden toiminta. Operaattori näkee SW Suite -käyttöliittymästä, koska laite on virheessä tai materiaalivirta pysähtyy. Operaattorin on käynnistettävä ja pysäytettävä laitteet sekä mahdollisesti muokattava yksiköitä tehdasasettelun valintaikkunassa tilanteen korjaamiseksi. Operaattori voi myös säätää tuotteiden parametreja (sisäisiä tietoja).

Taso 3: Tason työtehtävä on varmistaa, että kaikki tilaukset tulevat kerätyiksi ja materiaali on oikeassa paikassa oikeaan aikaan. Operaattorin on ymmärrettävä koko järjestelmän toiminta. Operaattori monitoroi SW Suite –käyttöliittymän kautta järjestelmään luotuja ja kerättyjä tilauksia. Operaattori säätää järjestelmän parametreja sekä käsittelee mahdollisia tuotteiden puutteita. Operaattori voi myös päättää tilausten poimimisjärjestyksestä vapauttamalla ne poimintaan, etenkin laatikoiden käsittelyssä.

Taso 4: Tason työtehtävä on hallita käyttöoikeuksia ja pystyä käynnistämään ja pysäyttämään palvelimessa taustapalveluja tarvittaessa. Operaattorin on ymmärrettävä koko järjestelmä. Yleensä tason 3 ja 4 operaattori on sama henkilö.

6.3 LDAP-palvelinohjelmat

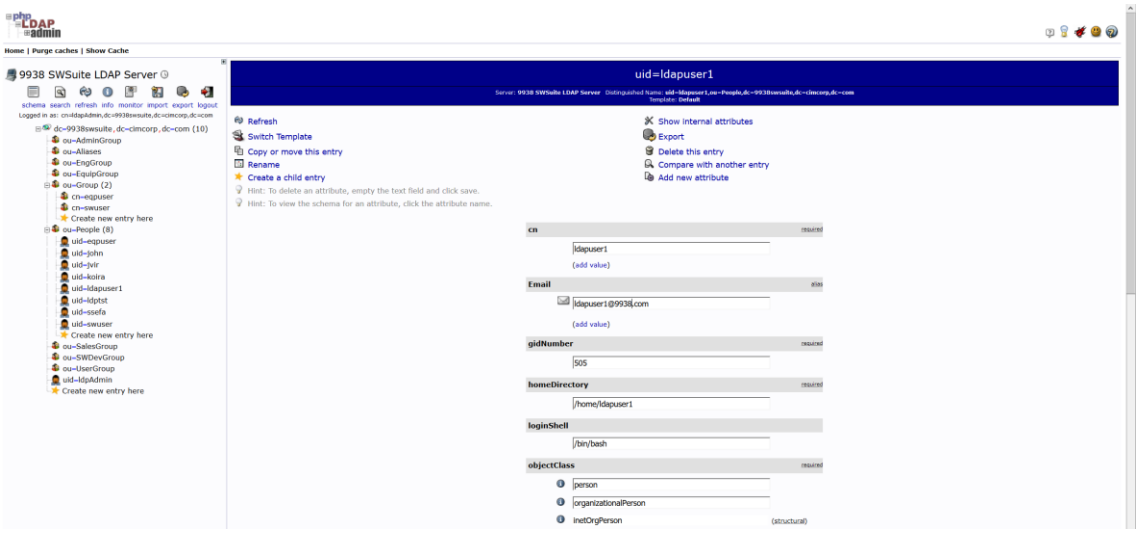
LDAP-järjestelmä voi vaikuttaa vaikealta hallita, jos käyttäjällä ei ole tarpeeksi tietoa käytettävissä olevista työkaluista ja LDAP:n edellyttämistä tiedoista ja menetelmistä. Tässä luvussa esitellään muutama LDAP-käyttöliittymä, joita voidaan käyttää vuorovaikutuksessa LDAP-hakemistopalvelimen kanssa.

6.3.1 PhpLDAPadmin

PhpLDAPadmin-sovellus on kevyt LDAP-palvelimen ylläpidon työkalu, jonka avulla voidaan toteuttaa muun muassa organisaatioiden ja käyttäjien hallinta selaimen graafisen käyttöliittymän kautta. PhpLDAPadmin (tunnetaan myös nimellä PLA) on web-pohjainen LDAP-käyttöliittymä. Ohjelma tarjoaa kaikkialla käytettävän ja monikielisen hallinnan LDAP-palvelimelle. LDAP:in hierarkkinen puunäkymä ja hakutoiminto auttavat LDAP-hakemiston selauksessa ja hallinnassa. Koska kyseessä on web-sovellus, LDAP-selain toimii monilla alustoilla, joten LDAP-palvelinta voidaan hallita helposti missä tahansa paikassa. PhpLDAPadmin-käyttöliittymän etusivu on esitetty kuvassa 11. [34]

PhpLDAPadmin-ohjelman ominaisuudet: [34]

- LDAP-puun selain
- Mallipohjainen merkinnän luonti, muokkaus ja poisto
- LDAP-merkintöjen kopiointi
- Kokonaisen puun kopiointi/poisto
- LDAP-merkinnän poisto
- Kuvatietojen tarkastelu ja muokkaus
- LDAP-haut (sekä yksinkertaiset että edistyneet)
- LDIF-tiedostojen vienti ja tuonti
- LDAP-merkinnän uudelleen nimeäminen
- Käyttäjän salasanojen hallinta (tukee seuraavia salauksia sha, crypt, md5, blowfish, md5crypt)



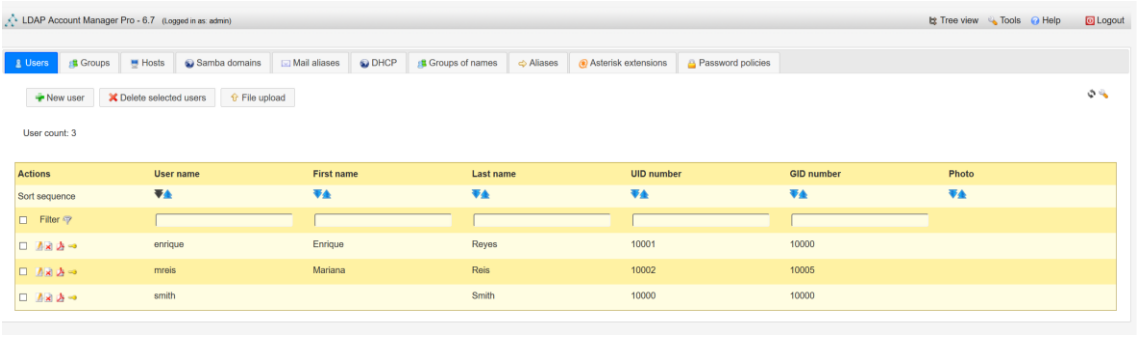
Kuva 11 PhpLDAPadmin käyttöliittymä

6.3.2 LDAP Account Manager

LDAP Account Manager (käytetään myös nimeä LAM) on web-pohjainen LDAP-hakemistoon tallennettujen merkintöjen (esimerkiksi käyttäjien ja ryhmien) hallintaan tarkoitettu ohjelma. LAM:n tarkoituksena on tehdä LDAP-hallinta mahdollisimman helpoksi käyttäjälle. Ohjelma tiivistää LDAP:n tekniset yksityiskohdat ja antaa niille, joilla ei ole teknistä taustaa, mahdollisuuden hallita LDAP-merkintöjä. Tarvittaessa pääkäyttäjät voivat silti suoraan muokata LDAP-merkintöjä integroidun LDAP-selaimen kautta. LDAP Account Manager -käyttöliittymän etusivu on esitetty kuvassa 12. [35]

LDAP Account Manager ominaisuudet:

- Puunäkymän lisäksi välilehdillä eri tasoisten käyttäjien näkymät
- Ylläpitäjien hallintatyökalua
- Käyttäjät voivat muokata omia tietojaan, joita ovat esimerkiksi salasana, osoite ja puhelinnumero
- salasana itse nollautuu
- käyttäjän itsensä rekisteröinti
- tuki mukautetulle LDAP-skeemalle [35]

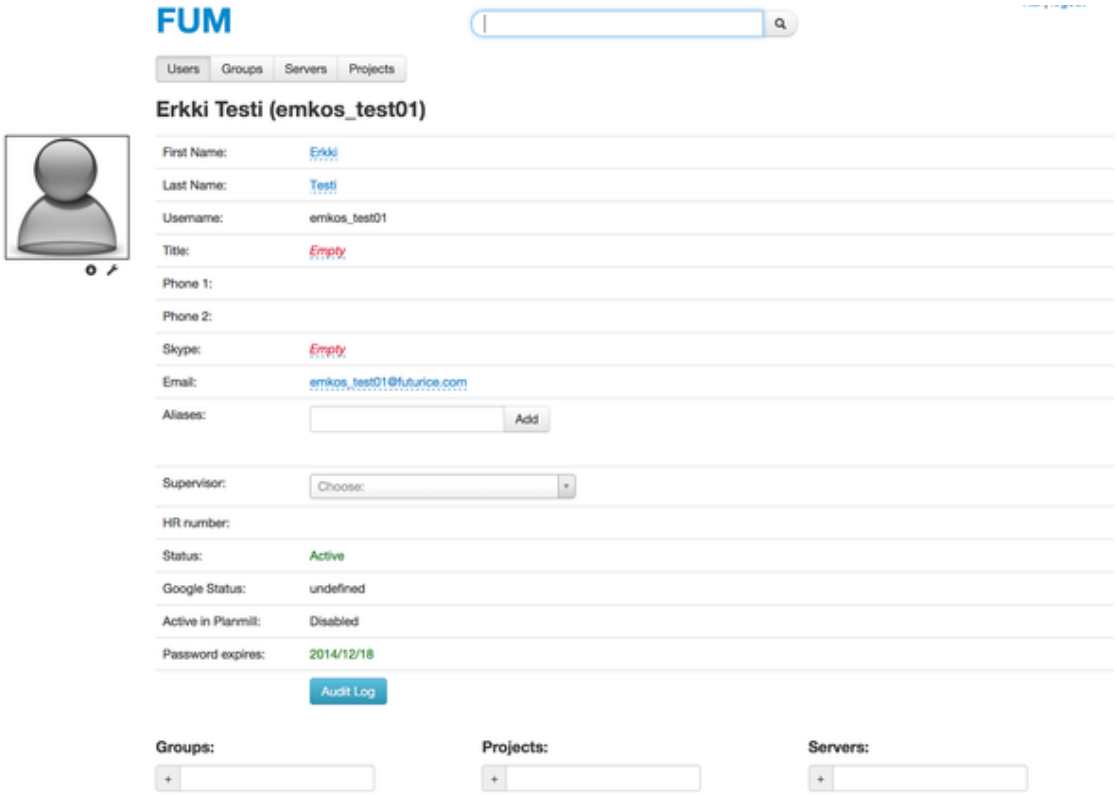


Kuva 12 LDAP Account Manager

6.3.3 FUM

FUM on LDAP:n käyttäjänhallintajärjestelmä. FUM:n avulla on helppo käsitellä tietoja työntekijöistä, projekteistaan ja palvelimistaan. LDAP on hyvä protokolla käyttäjähallinnalle, mutta siihen tarvitaan käyttäjäystävällinen kerros. Yksi FUM:in vahvuuksista on se, että se antaa käyttäjille paljon vapautta tietojensa suhteen. [36]

FUM on integroitu LDAP:iin, mutta sillä on myös oma tietokantansa. Tämä vähentää vuorovaikutusta LDAP:n kanssa ja sallii työntekijöihin liittyvien lisätietojen tallentamisen. FUM:illa on myös sovellusliittymä, jonka avulla työntekijöitä voidaan helposti integroida eri palveluihin. FUM-käyttöliittymän etusivu on esitetty kuvassa 13. [36]



Kuva 13 FUM

PhpLDAPadmin palvelee käyttötarkoitustaan ja on ominaisuuksiltaan riittävä käyttäjähallinnan tarpeisiin. PhpLDAPadmin oli käytössä joustava ja organisaation skeeman luonti sekä resurssiryhmien hallinta tarpeiden mukainen. Lisätietoja PhpLDAPadmin-käyttöliittymän hallinnasta on esitetty tämän työn liitteissä, jossa on esitetty PhpLDAPadmin-ohjelman lyhyt käyttöohje.

7. KÄYTTÄJÄN AUTENTIKOINNIN TOTEUTUS

Tässä luvussa käsitellään diplomityön käyttäjän autentikoinnin toteutus RFID-teknologiaa hyödyntäen. WCS-työasemalla USB-liitännäisen RFID-lukijan lukijan toiminto on lukea käyttäjän tunniste, joka välitetään web-sovelluksen kautta LDAP-palvelimella tunnistamista varten. LDAP on laajennettu tukemaan MIFARE-kortin sarjanumeroiden tallennusta suoraan (objectClass uccDispenseAccount ja attribuutti uccDispenseMIFARE). Tässä diplomityössä tunnisteen sarjanumero on attribuutti employeeNumber (objectClass inetOrgPerson). [37]

Kuva 14 RFID lukija ja Mifare Classic -tunniste

Diplomityössä käytetty RFID-lukija on saksalaisen FEIG Electronicin valmistama CPRR40.30-USB. Lukija on yhteensopiva Mifare Desfire EV1 -standardin mukaisten tunnisteiden kanssa. Käytössä ollut lukija ja tunniste on esitetty kuvassa 14. [38]

Lukijan konfigurointi- ja ohjauskomennot on tarkoitettu lukijan mukauttamiseen käytössä olevaan sovellusalueeseen asynkronisen rajapinnan kautta. Lukijan konfigurointiparametrit tallennetaan lukijan EEPROM-muistiin, josta ne käynnistyksen yhteydessä luetaan. [39]

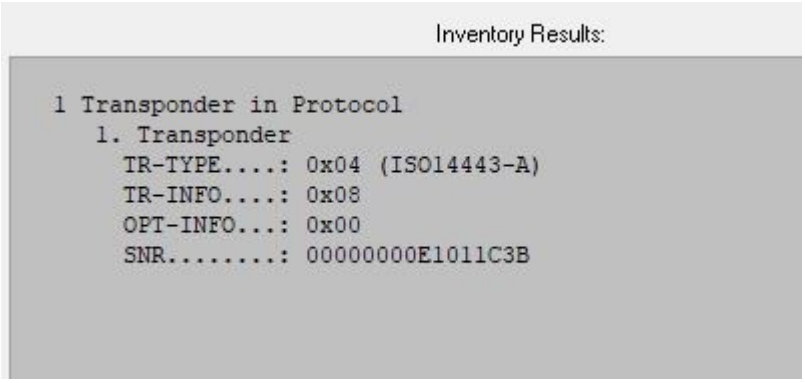
Tunnisteen toiminta testattiin tehdasolosuhteisiin suunnitella Panasonic-tabletilla, jonka monikosketusnäyttöä voidaan käyttää raskaiden käsineiden kanssa, ja joka sisältää RFID-lukijan.

7.1 Tunnisteen konfigurointi

MIFARE on NXP Semiconductorsin omistama tuotemerkki, jota käytetään etäluettavissa älykorteissa. MIFARE-korttien patentoidut ratkaisut perustuvat standardeihin, jotka määrittelevät etäluettavan älykortin toiminnallisuuden. Korttien ominaisuudet noudattavat standardia ISO/IEC 14443. MIFARE-kortin sisältö ja sille kirjoittaminen voidaan salata useilla avaimilla, mikä lisää ylimääräisen suojauksen kortinlukijan ja kortinlukuohjelmiston välille. [40]

MIFARE-tunnisteen yksilöllinen sarjanumero ja kortin muistisektoreille tallennettu tieto suojataan turva-avaimilla. Lukijaan liitetyn ohjelmointityökalun CPRStart 2018 avulla on mahdollista lukea ja muokata RFID-lukijan ja -tunnisteiden asetuksia.

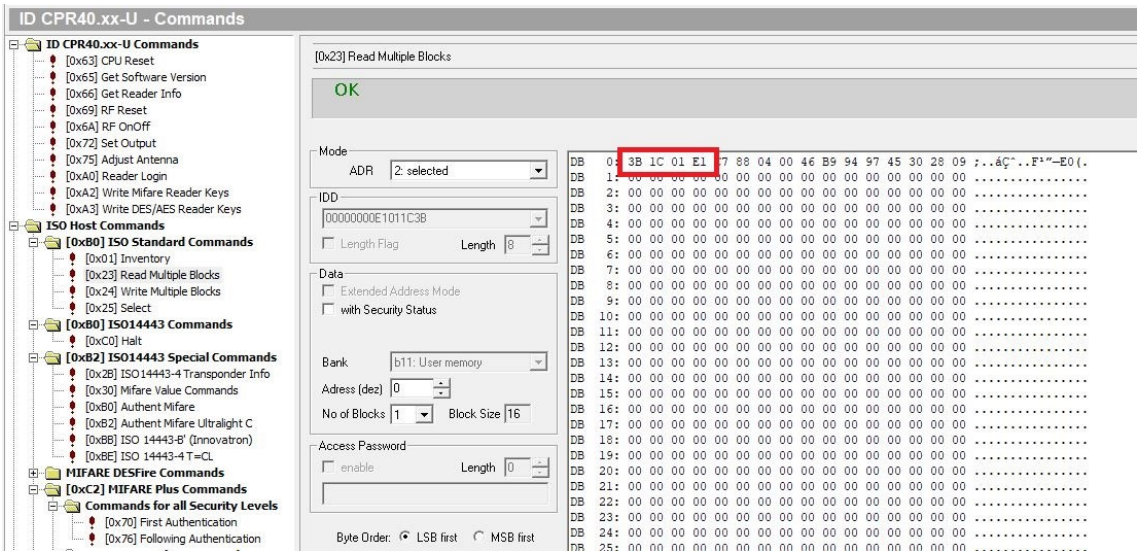
Komentoikkuna sisältää kaikki protokollat, jotka liittyvät lukijaan sekä komennot kommunikointiin tunnisteiden kanssa. Ennen tiedonsiirtoa tunnisteen kanssa yhteys avataan tunnisteelle Inventory-komennolla. Komento palauttaa tunnisteen tyypin ja sarjanumeron. Inventory-komennon palauttama tieto on esitetty kuvassa 15.



Kuva 15 Inventory-komennon palauttama tieto

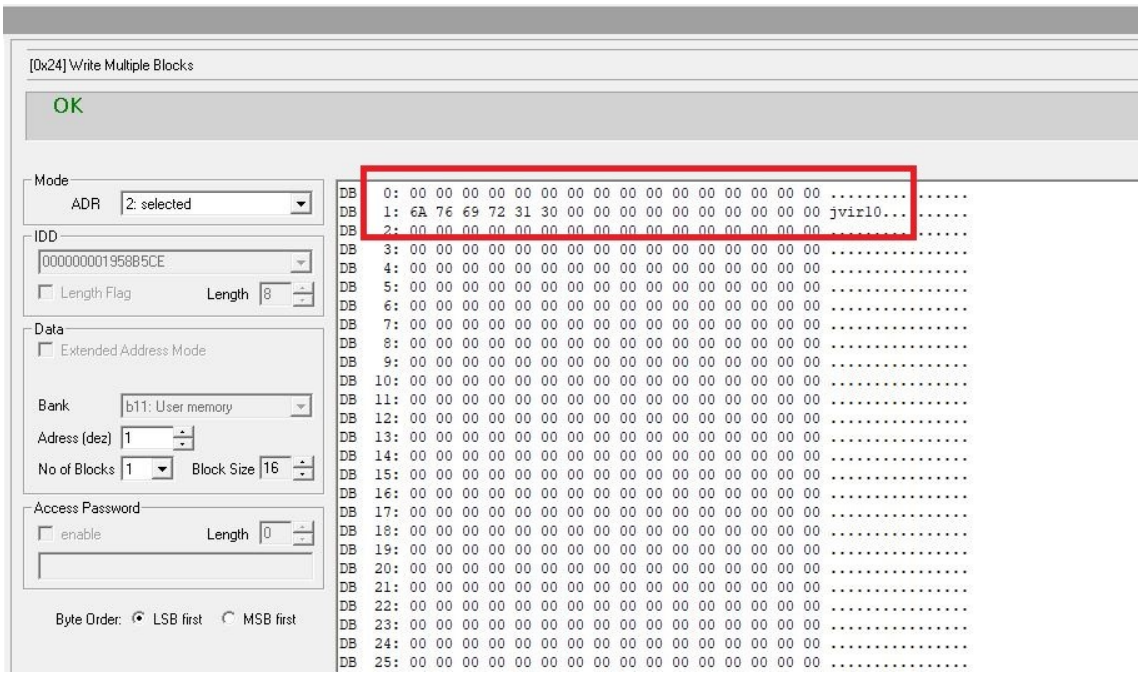
Tämän jälkeen mikä tahansa muu toimenpide, kuten datalohkojen lukeminen ja kirjoittaminen voidaan suorittaa tunnisteella. Select-komennolla nähdään korttityyppi. Read Multiple Blocks -komennolla saadaan näkyviin korttiin koodattu yksilöllinen tunniste sekä

kortille kirjoitetut datalohkot. Tässä työssä salattua sarjanumeroa käytetään käyttäjän tunnistautumisessa. MIFARE Classic tunnisteen sarjanumero data-alueella on esitetty kuvassa 16.



Kuva 16 MIFARE Classic tunnisteen sarjanumero

Write Multiple Blocks -komennolla voidaan kortin tyhjille sektoreille kirjoittaa haluttu data voi olla heksadesimaali- tai ASCII -muodossa, salattuna tai salaamattomana. MIFARE Classic tunnisteelle kirjoitettu data on esitetty kuvassa 17.



Kuva 17 MIFARE Classic tunnisteelle kirjoitettu data

7.2 Lukijan ja tunnisteen kuuntelun toteutus

Työssä käytettiin Javax.smartcardio-kirjasto, jonka avulla toteutettiin Java-ohjelma kommunikointi älykorttien kanssa. Paketti määrittelee Java-sovellusliittymän kommunikoinnin älykorttien kanssa käyttämällä ISO/IEC 7816-4 APDU -sovelluksia. Siten Java-sovellukset voivat olla vuorovaikutuksessa älykortilla toimivien sovellusten kanssa sekä tallentaa ja hakea tietoja kortille. [41]

Saatavilla olevien lukijoiden listaus:

```
private void retrieveTerminals() {
    List<CardTerminal> terminals = null;
    try {
        // show the list of available terminals
        TerminalFactory factory = TerminalFactory.getDefault();
        terminals = factory.terminals().list();
        System.out.println("Terminals: " + terminals);

    } catch (CardException e) {
        logger.error("{}", e.getMessage());
        Platform.runLater(() -> ClientErrorDialog.getInstance()
                .showClientError("error.rest.connection", "error.rest.message"));
    }

    if (terminals != null && !terminals.isEmpty()) new SmartCardManager(terminals);
}
```

Yhteyden muodostaminen tunnisteeseen:

```
public SmartCardManager(List<CardTerminal> terminals) {
    if (terminals != null) {
        for (CardTerminal terminal : terminals) {
            try {
                if (terminal.isCardPresent()) {
                    // establish a connection with the card
```

```
                Card card = terminal.connect("*");
                System.out.println("card: " + card);

                CardChannel channel = card.getBasicChannel();
                byte[] cmdAPDUGetCardUid = new byte[]{
                        (byte)0xFF, (byte)0xCA, (byte)0x00, (byte)0x00, (byte)0x00};

                ResponseAPDU respAPDU = channel.transmit(
                        new CommandAPDU(cmdAPDUGetCardUid));

                if(respAPDU.getSW1() == 0x90 && respAPDU.getSW2() == 0x00){

                    byte[] baCardUid = respAPDU.getData();

                    System.out.print("Card UID = 0x");
                    for(int i = 0; i < baCardUid.length; i++ ){
                        System.out.printf("%02X ", baCardUid [i]);
                    }

                    System.out.println("received: " + bytesToHex(baCardUid));
                    handleSubmit(bytesToHex(baCardUid));

                    card.disconnect(false);
                }
            }
            if (terminal.isCardPresent() == false) {
                System.out.println("*** Insert card");
            }
        } catch (CardException e) {
            e.printStackTrace();
        }
    }
  }

}
```

7.3 LDAP-käyttäjän todennus

LDAP-käyttäjän todennus on joko käyttäjänimen ja salasanan yhdistelmän tai RFID-kortin numeron validointiprosessi hakemistopalvelimen kanssa. Käyttäjän todentaminen LDAP-hakemistolla on kaksivaiheinen prosessi.

Ensimmäisessä vaiheessa luodaan yhteys LDAP-serverille:

```
public static DirContext connectToLDAP(String url, String user, String password){
  Hashtable<String, String> env = new Hashtable<>();
  env.put(Context.INITIAL_CONTEXT_FACTORY,
"com.sun.jndi.ldap.LdapCtxFactory");
  env.put(Context.PROVIDER_URL, url);
  env.put(Context.SECURITY_AUTHENTICATION,"simple");
  env.put(Context.SECURITY_PRINCIPAL, user);
  env.put(Context.SECURITY_CREDENTIALS,password);
  try {
    // Create initial context
    DirContext ctx = new InitialDirContext(env);
    logger.info("Connected to LDAP server.");
    return ctx;
  } catch (Exception e) {
    logger.error("{}", e.getMessage());
    return null;
  }
}
```

Hakemiston käyttäjä tunnistetaan yksilöllisellä tunnuksella (DN), joka muistuttaa hakemiston juuresta alkavaa polkumaista rakennetta:

uid = jvir, ou = people, dc=swsuite, dc=cimcorp, dc=com

Käyttäjän todennus LDAP-hakemistolla tapahtuu käyttäjän DN sekä salasanan avulla. Kirjautumislomakkeella käyttäjät yleensä kirjoittavat yksinkertaisen tunnisteen, kuten käyttäjänimen tai sähköpostiosoitteen sekä salasanan. Käyttäjän ei odoteta muistavan

hakemistonsa DN-osoitetta. RFID-tunnistaumisessa käyttäjä näyttää kortin RFID-lukijassa.

Käyttäjän nimi, sähköposti tai tunnisteen numero välitetään hakemistopalveluun, jossa suoritetaan haku käyttäjän nimen tai sähköpostiominaisuuksien tai kortin numeron perusteella, jotta löydetään vastaavan merkinnän DN. Hakemistopalvelut käyttävät erittäin tehokasta indeksointia ja välimuistiin tallentamista, joten haut ovat yleensä erittäin nopeita.

Kirjautuminen tunnisteella:

```
public static boolean smartCardLogin(String cardid) {
    String filter = "(&(objectClass=person)(employeeNumber="+ cardid + "))";
    SearchResult searchResult = search(cardid, filter);
    displayName = new
StringBuilder(searchResult.getAttributes().get(DISPLAY_NAME).toString());
    String filterRole = "(&(objectClass=groupofnames)(member="+
searchResult.getNameInNamespace() + "))";
    SearchResult searchResultRole = search(cardid, filterRole);
    userRole = new
StringBuilder(searchResultRole.getAttributes().get(USER_ROLE).toString());
    System.out.println("displayName " + displayName);
    try {
        setFullName(displayName.delete(0,13).toString());
        setRole(userRole.delete(0,4).toString());
        System.out.println(getRole());
        toggleLogin();
        return true;
    } catch (Exception e) {
        logger.error("{}", e.getMessage());
    }
    return false;
}
```

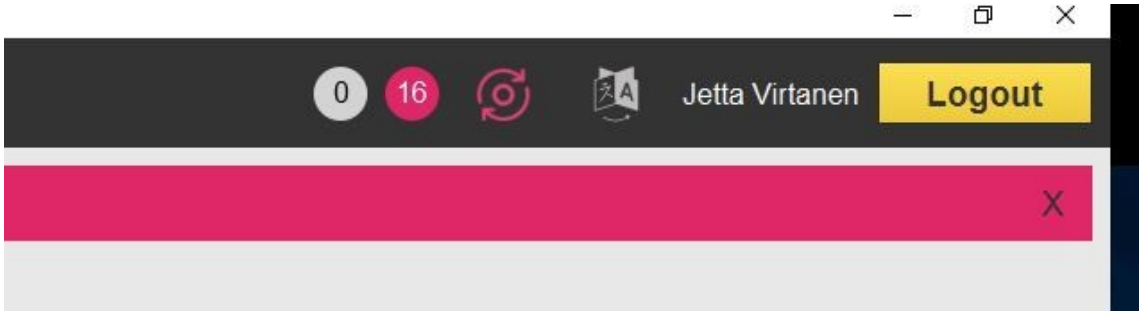
Haettavat hakemistomääritteet määritetään hakulauseiden ja muiden parametrien avulla kuten haun kohdehaara (base DN) sekä hakusuodatin (search filter). Attribuutit kuten

käyttäjänimi, sähköposti, tunnistenumero, joilla käyttäjä sisäänkirjautuu, on oltava uniikkeja. Jos kahdella merkinnällä löydetään sama tunnisteattribuutti, esimerkiksi sähköpostiosoite, todennus hylätään.

```
public static SearchResult search (String username, String filter){
    DirContext context = connectToLDAP(URL, ADMIN, PASS);

    System.out.println("username 1 " + username);
    SearchControls ctls = new SearchControls();
    ctls.setSearchScope(SearchControls.SUBTREE_SCOPE);

    String search = "dc=9938swsuite,dc=cimcorp,dc=com";

    try {
        NamingEnumeration<SearchResult> answer = context.search(search, filter, ctls);
        if (answer == null || !answer.hasMore()) {
            System.out.println("No result found");
            return null;
        }

        SearchResult searchResult;
        searchResult = answer.nextElement();
        System.out.println(searchResult.getNameInNamespace());
        //make sure there is not another item available, there should be only 1 match
        if(answer.hasMoreElements()) {
            System.err.println("Matched multiple users for the username: " + username);
        }
        context.close();
        return searchResult;
    } catch (NamingException e){
        logger.error("{}", e.getMessage());
    }

    return null;
}
```

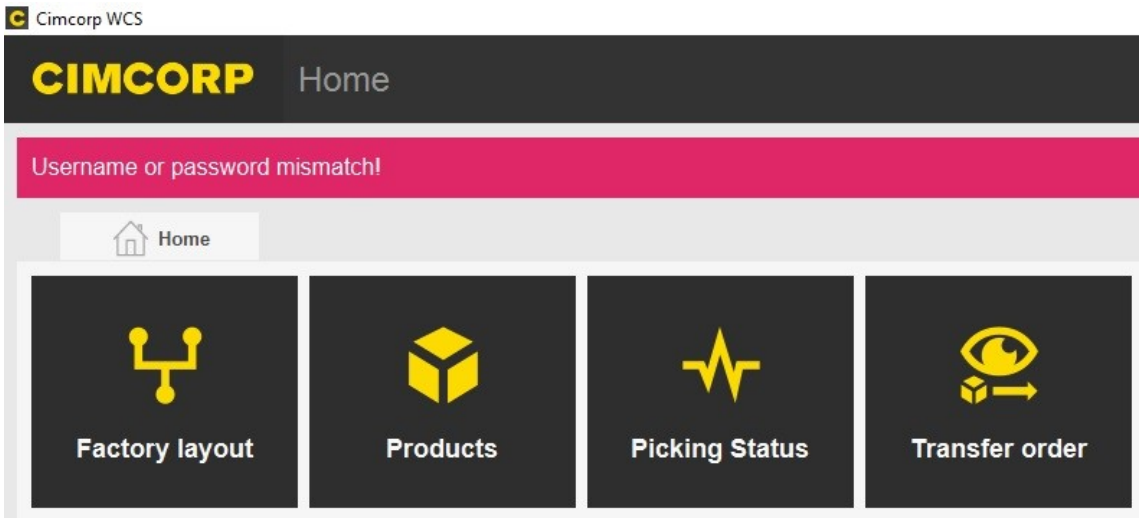
Tulee myös varmistaa, että jokaisella käyttäjällä, jonka odotetaan kirjautuvan sisään, on määritetty määrite tunnistettavalle määritteelle. Esimerkiksi, jos käyttäjät kirjautuvat sisään sähköpostiosoitteellaan, varmistetaan, että kaikilla tileillä on määritetty sähköpostiominaisuus. Muuten todennus epäonnistuu.

Käyttäjän todennuksen jälkeen LDAP-hakemistopalvelu palauttaa käyttäjän nimen, ryhmän ja roolin. Palautetun roolin perusteella voidaan määritellä käyttäjän näkymä. Sisäänkirjautuneen käyttäjän nimi näkyy käyttöliittymässä kuvan 18 mukaisesti.



Kuva 18 Sisäänkirjautuneen käyttäjän nimi

Mikäli käyttäjätunnus, salasana tai kortin sarjanumero ei täsmää LDAP-hakemistopalvelimen tietoihin tai todennuspalvelimeen (LDAP-palvelin) ei saada yhteyttä, niin sisäänkirjautumissivulle ilmestyy asiaan liittyvä virheviesti kuvan 19 mukaisesti.



Kuva 19 Autentikoinnin virheviesti

8. TULOKSET JA JOHTOPÄÄTÖKSET

Käyttäjähallinta voi luoda yrityksille ja organisaatioille haasteita. Työntekijöihin liittyvien tietojen tallentaminen on EU:n tuoreen tietosuoja-asetuksen GDPR:n (General Data Protection Regulation) mukaan henkilörekisteri ja yritysten toiminnan tulee olla uusien tietosuojamääräysten mukainen. Toimiva käyttäjähallinta edistää myös yrityksen toimintaa palvelemalla loppukäyttäjää, vähentämällä kirjautumiseen tarvittavaa aikaa ja parantamalla tietoturvaa. Cimcorp Oy:n varastonhallintajärjestelmien käyttöliittymissä on perinteisesti ollut käytössä sisäänrakennettu käyttäjähallinnan toteutus. Asiakkaiden määrän kasvu on kasvattanut käyttäjätunnusten ja -oikeuksien ylläpidon määrää. Diplomityön tarkoituksena oli tutkia, miten käyttäjän autentikointi ja käyttäjätunnusten hallinnointi voidaan toteuttaa yleisellä teknologialla erillään olemassa olevasta varastonhallintajärjestelmästä.

Tutkimuksen päätavoitteena oli määrittää mahdollisuus käyttää teknologiaa varaston hallintajärjestelmässä ja toteuttaa Cimcorp Oy:n varastonhallintakäyttöliittymään käyttäjän autentikointi RFID-teknologialla. Työn tuloksena käyttäjän on mahdollista kirjautua varastonhallintajärjestelmän käyttöliittymäsovellukseen RFID-tunnisteen avulla, jolloin käyttöliittymän näkymä määräytyy käyttäjälle asetetun roolin mukaiseksi. RFID-tunniste määrää myös tuotantolaitoksen alueen tai laitteen, jossa käyttöliittymä toimii. Järjestelmän ilmoittaa, mikäli jonkin toiminnan suorittaminen jää kiinni käyttöoikeuksista, ja antaa mahdollisuuden samassa yhteydessä vaihtaa käyttäjää.

Diplomityössä tutkittiin myös kaupallisia web-sovelluksia, joiden avulla pystytään rekisteröimään ja ylläpitämään soveltuvia RFID-tunnisteita asiakkaan hakemistopalvelimelle. Toteutukseen valittiin alustasta riippumaton avoimen lähdekoodin OpenLDAP-hakemistopalvelin. LDAP on yksi apumenetelmä keskitettyyn käyttäjähallintaan. LDAP tarjoaa standardoidun tiedonsiirron sekä paikallisille että etäyhteyksille. LDAP-toteutus on mahdollista korvata ilman, että se vaikuttaa ulkoiseen rajapintaan, joten LDAP-käyttäjiä ja -palvelimia voidaan kehittää itsenäisesti.

LDAP-hakemistopalvelun käyttö on helppo, yksinkertainen ja tehokas tapa keskittää käyttäjähallinta ja -autentikointi yrityksen sisällä. Yksinkertainen protokolla ja toimintavarmuus ovat LDAP-hakemistopalvelun vahvoja puolia. Tässä diplomityössä esitellyillä

ratkaisulla on mahdollista toteuttaa varastohallintajärjestelmän käyttöliittymän autentikointi asiakkaan omaa LDAP-hakemistopalvelua hyödyntäen. Hakemistopalvelun käytöllä voidaan purkaa käyttäjien validointityökuormat ja saavuttaa mahdollisesti suorituskyvyn parannuksia. LDAP on myös helppo jakaa useille palvelimille. Käyttäjillä voi luoda hyvinkin monimutkainen ryhmäjäsenyys, ja minkä tahansa objektiluokan tai määritteen käyttöoikeudet voidaan mukauttaa.

Työntekijöiden sisäänkirjautuminen ja kirjautuminen ulos erillisellä tunnisteella on nopeampaa ja helpompaa vaihtelevissa tehdasolosuhteissa. Tunnisteen käytön myötä riski jaetuista salasanoista tai tileistä poistuu. Tunnisteen käyttö tarjoaa asiakkaalle tarkastusketjun sekä mahdollisuuden hyödyntää jo olemassa olevia tunnisteita esimerkiksi henkilökortteja.

Diplomityön esittämän toteutuksen haasteena on, että asiakkaan kannalta edulliseen RFID-tekniikkaan pohjautuvissa autentikoinnissa ei voida välttämättä tuottaa tehokasta todennusta tai salausta. Järjestelmät, joiden tietoturva on riittävä, ovat kustannuksiltaan korkeammat. RFID-järjestelmien käytössä on panostettava yrityksen ja yksilön yksityisyyden takaamiseen, estettävä tunnisteiden laiton seuranta, luvaton profilointi, kloonaaminen ja laiton lukeminen/kirjoittaminen. Suljetussa tuotantoympäristössä toteuttaminen on kuitenkin melko vaivatonta eivätkä tietoturvariskit ole niin suuria.

LDAP:in käytössä on lisäksi huomioitava, että se ei ole relaatiotietokanta, joten se ei toteuta palautusta epäonnistuneista toiminnoista. LDAP ei ole tiedostojärjestelmä, joka voidaan lukita tai sieltä voidaan etsiä suuria määriä tietoa. LDAP on optimoitu lukemiseen ei kirjoittamiseen. LDAP ei ole hyödyllinen ilman sovelluksia.

Tässä diplomityössä ei käsitelty tarkemmin varastohallintajärjestelmän käyttöliittymän toteutusta käyttäjän roolin tai ryhmän mukaan. Sisäänkirjautumisen yhteydessä LDAP-palvelimelta haettujen, käyttäjää koskevien attribuuttien arvojen on mahdollista määrätä käyttäjän rooli ja ryhmä. Käyttäjälle asetetusta roolista riippuen käyttöliittymän aloitusnäkymän sisältö ja käyttäjän oikeudet voitaisiin mukauttaa rooliryhmän mukaiseksi. Rooliryhmien toteutuksen lisäksi RFID-teknologin laajempi hyödyntäminen voisivat mahdollisuuksien mukaan olla tulevien opinnäytetöiden aiheina.

LÄHTEET

[1] Cimcorp Oy:n internet sivut, saatavilla HTML-muodossa, https://www.cimcorp.com/fi/cimcorp/cimcorp-konserni, viitattu 19.2.2019

[2] Avoine G. & Oechslin P, A Scalable and Provably Secure Hash Based RFID Protocol, 2nd IEEE International Workshop on Pervasive Computing and Communication Security, https://ieeexplore.ieee.org/abstract/document/1392812, 2005.

[3] White, Gareth & Gardiner, Georgina & Prabhakar, Guru & Abd Razak, Azley, A Comparison of Barcoding and RFID Technologies in Practice. Journal of Information, Information Technology and Organizations, https://www.researchgate.net/publication/279650706_A_Comparison_of_Barcoding_and_RFID_Technologies_in_Practice, 2007.

[4] Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&cad=rja&uact=8&ved=2ahUKEwirwO7ar_7mAhWEyKYKHRTdD-LUQFjAHegQIARAC&url=https%3A%2F%2Fwww.iacr.org%2Fbooks%2F2010_ws_Anderson_SecurityEngineering.pdf&usg=AOvVaw11t4osz7RFD-qxQePPo34t, The Second Edition (2008).

[5] Yu-Yi Chen and Meng-Lin Tsai, The Study on Secure RFID Authentication and Access Control, https://www.intechopen.com/books/current-trends-and-challenges-in-rfid/the-study-on-secure-rfid-authentication-and-access-control, 2011.

[6] Paul A. Grassi, Michael E. Garcia, James L. Fenton, NIST Special Publication 800-63-3, Digital Identity Guidelines, saatavilla HTML-muodossa https://pages.nist.gov/800-63-3/sp800-63-3.html, revision 3, 2017.

[7] Dawn M. Turner, Digital Authentication - the basics, saatavilla HTML-muodossa https://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics, 2016.

[8] Luis Balbas, Digital authentication - factors, mechanisms and schemes, saatavilla HTML-muodossa https://www.cryptomathic.com/news-events/blog/digital-authentication-factors-mechanisms-schemes, 2017.

[9] David Y. Zhang, Anil K. Jain, Biometric Authentication, 2004.

[10] Paul A. Grassi , James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, Justin P. Richer, NIST Special Publication 800-63B, Digital Identity Guidelines, saatavilla HTML-muodossa https://pages.nist.gov/800-63-3/sp800-63b.html#sec8, 2017.

[11] Shin Bongsik, A Practical Introduction to Enterprise Network and Security Managemen, 2017.

[12] Syed A. Ahson, Mohammad Ilyas, RFID Handbook: Applications, Technology, Security, and Privacy, 2008.

[13] Tania Martin, Privacy in RFID Systems, https://dial.uclouvain.be/pr/boreal/object/boreal:132580, 2013.

[14] International Organization for Standardization. ISO/IEC 18000: Information technology - Radio frequency identification for item management, 2008.

[15] Klaus Finkenzeller, RFID Handbook, Second Edition, 2003.

[16] OECD, RFID Guidance and Reports, OECD Digital Economy Papers, https://doi.org/10.1787/230334062186, No. 150, OECD Publishing, 2008.

[17] Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, Ted Phillips, Guidelines for Securing Radio Frequency Identification (RFID) Systems, 2007.

[18] Sviatoslav Edelev, Towards a Lightweight, Secure, and Untraceable RFID Authentication Protocol, PhD Theses, 2015.

[19] Syed Ahson and Mohammad Ilyas, RFID handbook : applications, technology, security, and privacy, 2008.

[20] Oracle Corporation 2017, saatavilla HTML-muodossa https://docs.oracle.com/cd/E19396-01/817-7619/intro.html, viitattu 19.7.2019.

[21] LDAP for Rocket Scientists, Version 0.01.19, 2018, http://www.zytrax.com/books/ldap/

[22] OpenLDAP 2.4 Administrator's Guide, The OpenLDAP Foundation, https://www.openldap.org/doc/index.html, 1998-2012

[23] Timothy Howes, Mark C. Smith Gordon S. Good, Understanding and Deploying LDAP Directory Services, 2003.

[24] Brian Arkills, LDAP Directories Explained: An Introduction and Analysis, 2003.

[25] Active Directory Collection, Microsoft, saatavilla HTML-muodossa https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780036(v=ws.10)?redirectedfrom=MSDN#w2k3tr_ad_over_qbjd, 19.11.2014, viitattu 31.5.2019.

[26] OpenLDAP Public License for 2.4.48, saatavilla HTML-muodossa https://www.openldap.org/software/release/license.html, viitattu 31.5.2019

[27] Paul Watters, Solaris 8 Administrator's Guide, 2002.

[28] Oracle8i Integration Server Overview, Release 3 (8.1.7), https://docs.oracle.com/cd/A87860_01/doc/ois.817/a83729/adois09.htm, viitattu 5.9.2019

[29] K. Zeilenga, RFC 4512, OpenLDAP Foundation, saatavilla HTML-muodossa, https://tools.ietf.org/html/rfc4512, viitattu 14.11.2019.

[30] Brad Marshall, LDAP Theory and Management, http://www.freebookcentre.net/special-books-download/LDAP-Theory-and-Management-.html, 2014.

[31] Tuttle S., Ehlenberger A., Gorthi R., Leiserson J., Macbeth R., Owen N., Ranahandola S., Storrs M. and Yang C., Understanding LDAP Design and Implementation, http://www.redbooks.ibm.com/abstracts/sg244986.html?Open, International Technical Support Organization, IBM Redbook, 2004.

[32] Oracle JAVA documentation, saatavilla HTML-muodossa https://docs.oracle.com/javase/tutorial/jndi/ldap/auth_mechs.html, Oracle 2019

[33] Ed R. Harrison, RFC 4513, OpenLDAP Foundation, saatavilla HTML-muodossa, https://tools.ietf.org/html/rfc4513, viitattu 14.11.2019.

[34] PhpLDAPadmin, versio 8.4.2013, saatavilla HTML-muodossa http://phpldapadmin.sourceforge.net/wiki/index.php/Main_Page, viitattu 28.5.2019

[35] LDAP Account Manager manuaali, 2003 - 2019 Roland Gruber, saatavilla HTML-muodossa, https://www.ldap-account-manager.org/static/doc/manual/index.html

[36] FUM user management system for LDAP, https://github.com/futurice/futurice-ldap-user-manager

[37] LDAP for Rocket Scientists, Appendix E: LDAP - Object Classes and Attributes Version 0.01.19, 2018. http://www.zytrax.com/books/ldap/ape/

[38] Desktop Reader ID CPR40.30-x (13.56 MHz) Data Sheet, https://www.feig.de/en/products/identification/product/id-cpr4030/, Version Aug. 2016

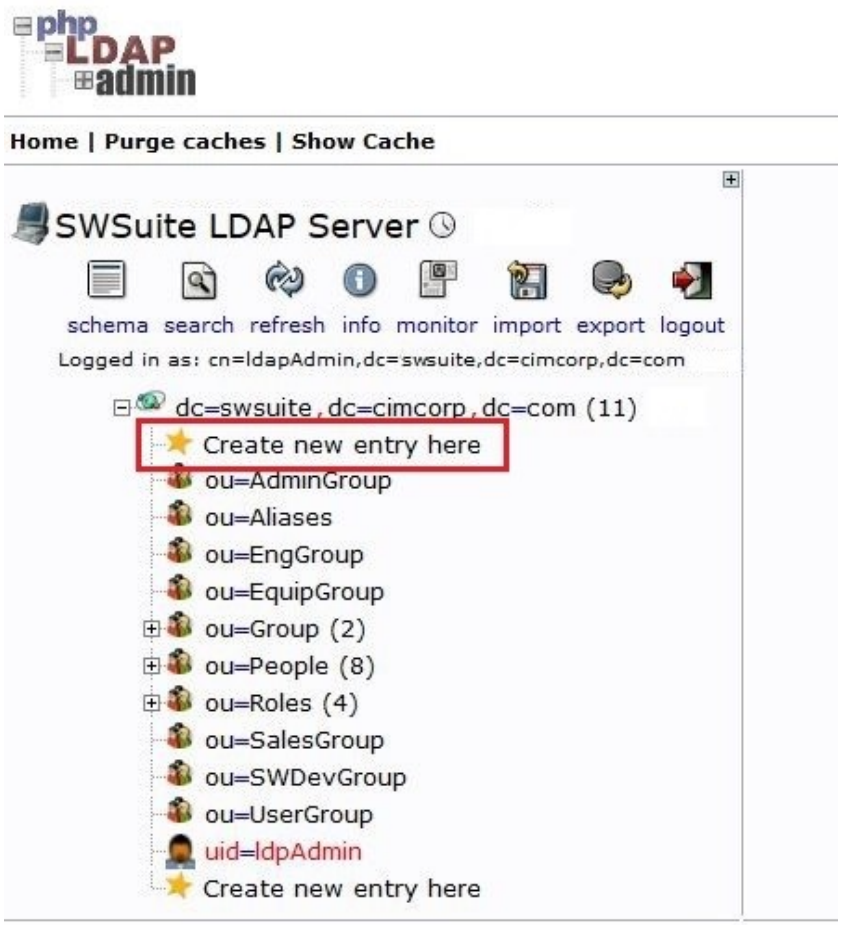
[39] ID CPR44.0x - Family RFID Reader Module with ISO14443-A and -B Support Manual, Version 03.02.00

[40] AN11340 MIFARE Ultralight and MIFARE Ultralight EV1 Features and Hints, NXP Semiconductors, Rev. 3.1, 9 July 2018.

[41] Oracle JAVA documentation 2018, saatavilla HTLM-muodossa https://docs.oracle.com/javase/7/docs/jre/api/security/smartcardio/spec/javax/smartcardio/package-summary.html, viitattu 5.9.2019.

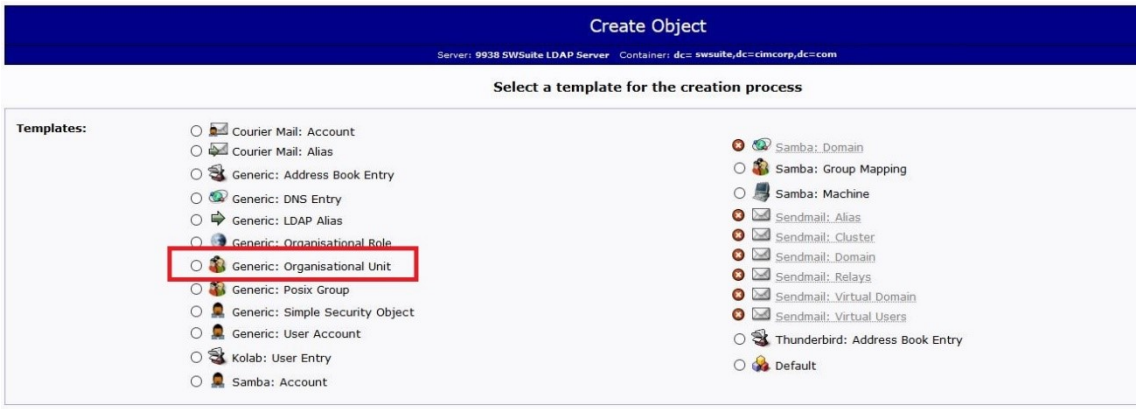
LIITTEET

LDAP koostuu tietomallin määrittelemistä osista. Kohdassa 9.1 esitetyn rakenteen mukaisesti tietomalliin lisätään organisaation ihmiset, ryhmät ja roolit. Yleisien organisaatioyksiköiden (OU = organizatiol unit) luomiseen käytetään organisaatioyksikön mallia, joka löytyy laajentamalla phpLDAPadmin-ohjelman palvelinluettelon ja napsauttamalla sitten ”Create new entry here” -kohtaa kuva 20.



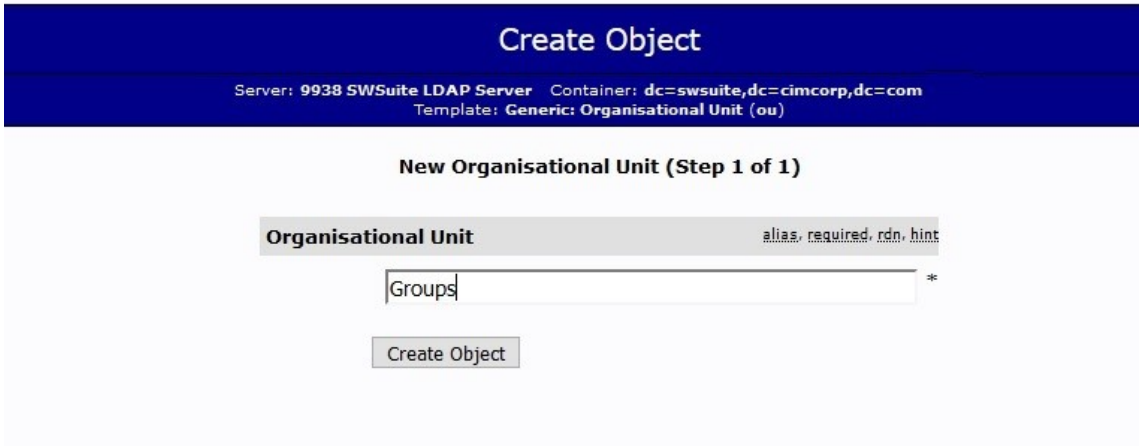
Kuva 20 Uuden merkinnän lisäys phpLDAPadmin

Merkinnän pohjaksi valitaan geneerinen organisatorinen yksikkö (Generic: Organisational Unit). Kuva 21.



Kuva 21 Templaten valinta

Ohjelmaan luodaan uusi OU nimeltään ”Groups”. Samoin lisätään OU-ryhmä käyttäjän rooleille ”Roles”-nimellä sekä käyttäjille ”People”-nimellä. Kuva 22. Roolien pohjaksi voidaan valita geneerinen organisatorinen rooli (Generic: Organisational Role).

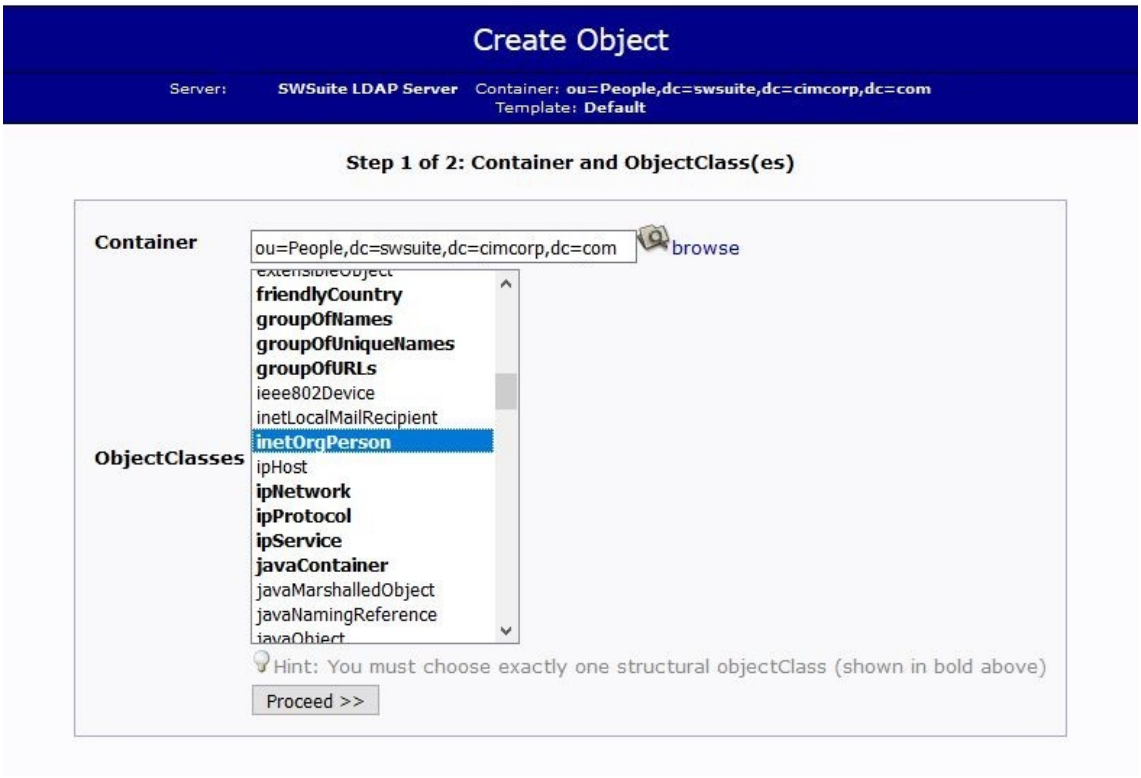


Kuva 22 Merkinnän nimeäminen

Luoduille organisatorisille yksiköille lisätään omat lapsimerkinnät esimerkiksi ryhmän ”People” alta laajentamalla palvelinluettelo ja napsauttamalla sitten ”Create new entry here” -kohtaa. Kuva 23.

Kuva 23 Lapsimerkinnän lisäys

Lapsimerkinnän objektiluokan valinta on esitetty kuvassa 24.

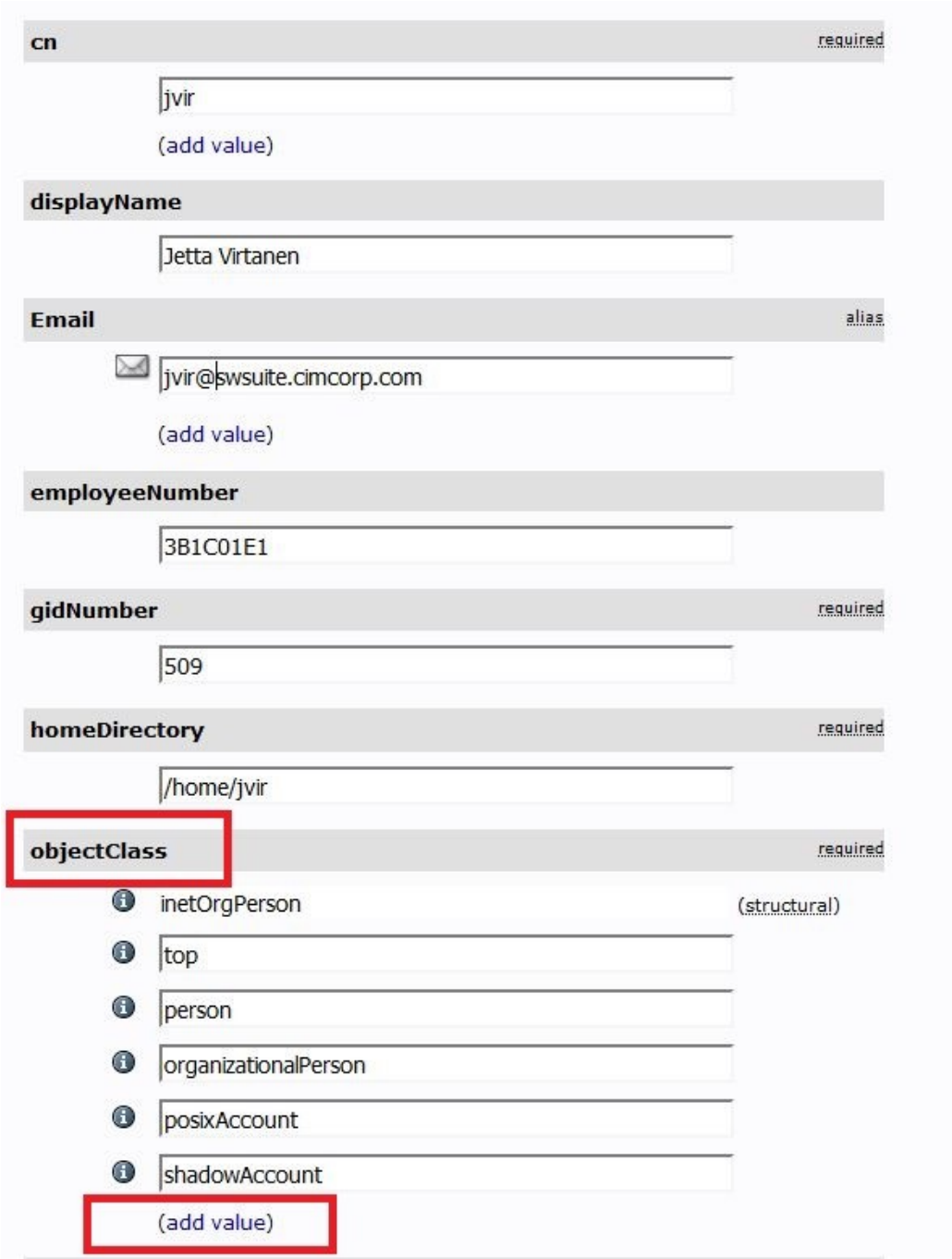


Kuva 24 Lapsimerkinnän objektiluokan valinta

Käytettävät objektiluokat voivat olla esimerkiksi seuraavanlaiset:

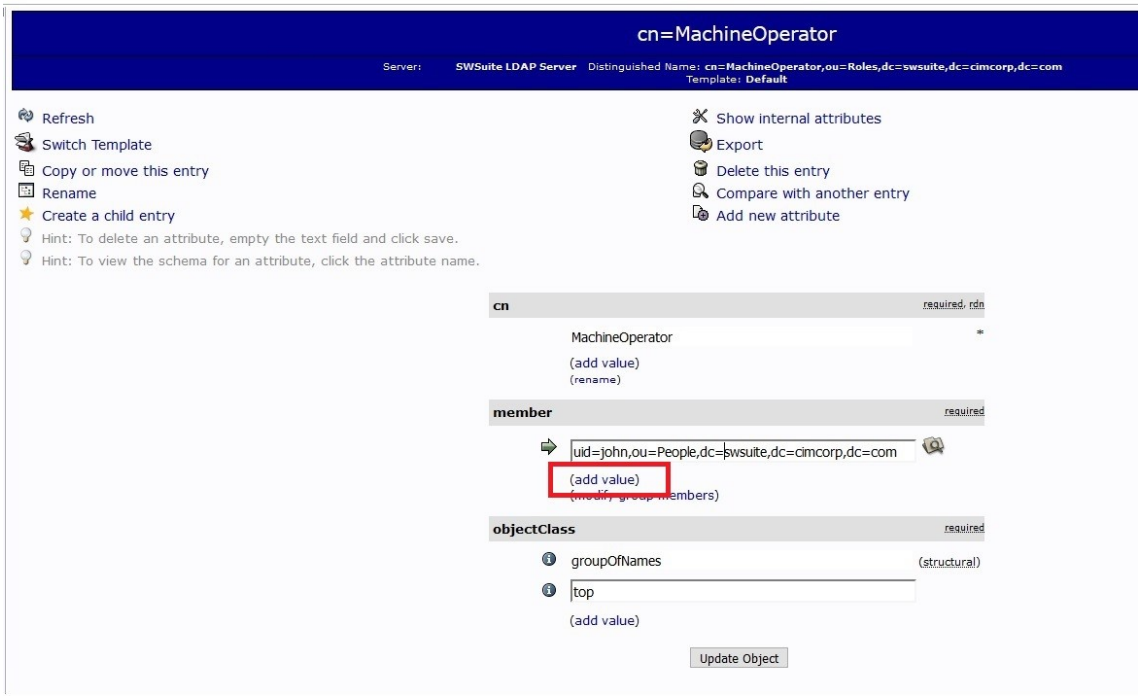
- Käyttäjät, objektiluokka inetOrgPerson
- Ryhmät, objektiluokka groupOfNames
- Roolit: objektiluokka groupOfNames

Objektiluokkien lisäys onnistuu merkinnän luonnin jälkeen attribuuttien tarpeen mukaan. Kuva 25.



Kuva 25 Objektiluokan lisäys lapsimerkintään

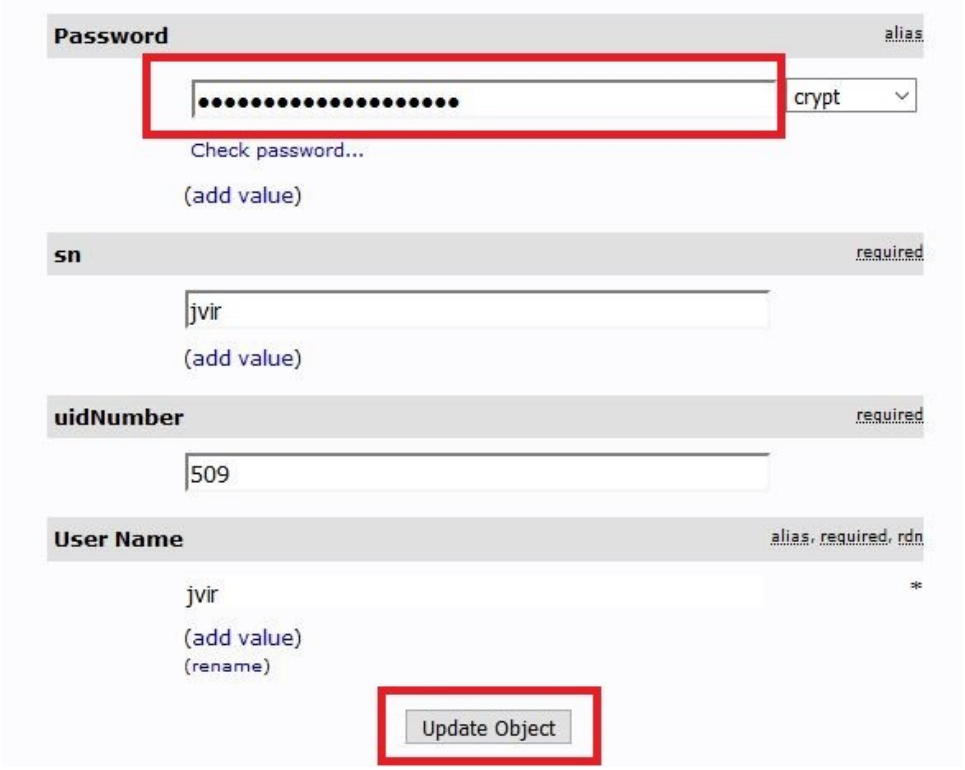
Rooli-yksikköön lisätään jäsenmerkintöinä henkilöt, jotka halutaan sitoa tietyn roolin alle. Henkilön lisäämiseksi ryhmään haluttu henkilö valitaan valikosta. Kuvat 26 ja 27.



Kuva 26 Jäsenen lisäys Roolit-ryhmään

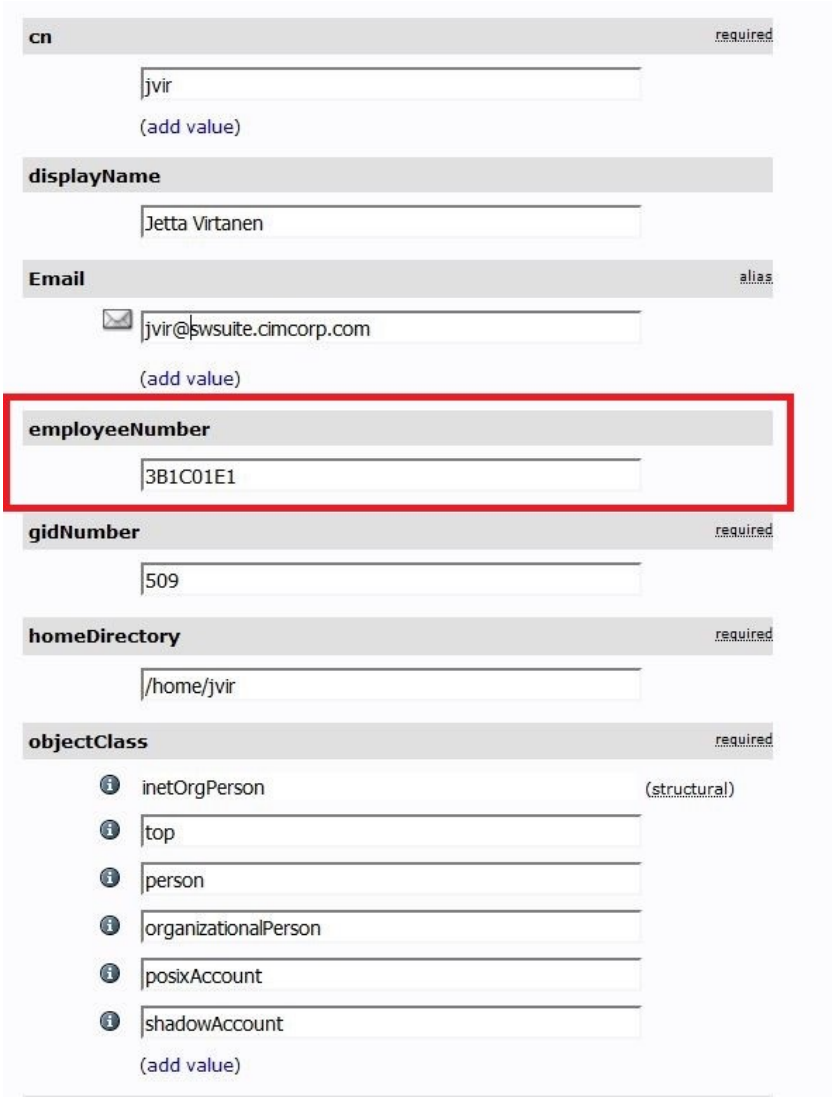
Kuva 27 Lisättävän jäsenen valinta

Henkilölle voidaan asettaa attribuuttiin ”Password” haluttu salasana. Muutokset tallennetaan ”Update Object” -napista. Kuva 28.



Kuva 28 Salasanan asetus ja tallennus

Käyttäjän todennus voi tapahtua asetetun salasanan ja esimerkiksi attribuutin ”uid” yhdistelmällä. Todennus RFID-kortilla tapahtuu kortin numeron perusteella. Valittuun attribuuttiin syötetään RFID-kortin yksilöllinen sarjanumero. Kuva 29.



Kuva 29 RFID-kortin numeron lisäys